Red Hat Enterprise Linux 9

Configuration des paramètres de base du système

Configurer les fonctions essentielles de votre système et personnaliser l'environnement de votre système

Last Updated: 2024-02-13

Red Hat Enterprise Linux 9 Configuration des paramètres de base du système

Configurer les fonctions essentielles de votre système et personnaliser l'environnement de votre système

Notice légale

Résumé

Effectuer les tâches d'administration de base du système, configurer les paramètres de l'environnement, enregistrer votre système et configurer l'accès au réseau et la sécurité du système. Administrer les utilisateurs, les groupes et les autorisations de fichiers. Utiliser les rôles système pour gérer l'interface des configurations système sur plusieurs systèmes RHEL. Utiliser systemd pour une gestion efficace des services. Configurer le protocole NTP (Network Time Protocol) avec chrony. Sauvegarder et restaurer votre système en utilisant ReaR.

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF

Red Hat s'engage à remplacer les termes problématiques dans son code, sa documentation et ses propriétés Web. Nous commençons par ces quatre termes : master, slave, blacklist et whitelist. En raison de l'ampleur de cette entreprise, ces changements seront mis en œuvre progressivement au cours de plusieurs versions à venir. Pour plus de détails, voir le message de notre directeur technique Chris Wright.

FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT

Nous apprécions vos commentaires sur notre documentation. Faites-nous savoir comment nous pouvons l'améliorer.

Soumettre des commentaires sur des passages spécifiques

1. Consultez la documentation au format **Multi-page HTML** et assurez-vous que le bouton **Feedback** apparaît dans le coin supérieur droit après le chargement complet de la page.
2. Utilisez votre curseur pour mettre en évidence la partie du texte que vous souhaitez commenter.
3. Cliquez sur le bouton **Add Feedback** qui apparaît près du texte en surbrillance.
4. Ajoutez vos commentaires et cliquez sur **Submit**.

Soumettre des commentaires via Bugzilla (compte requis)

1. Connectez-vous au site Web de Bugzilla.
2. Sélectionnez la version correcte dans le menu **Version**.
3. Saisissez un titre descriptif dans le champ **Summary**.
4. Saisissez votre suggestion d'amélioration dans le champ **Description**. Incluez des liens vers les parties pertinentes de la documentation.
5. Cliquez sur **Submit Bug**.

CHAPITRE 1. MODIFIER LES PARAMÈTRES DE BASE DE L'ENVIRONNEMENT

La configuration des paramètres de base de l'environnement fait partie du processus d'installation. Les sections suivantes vous guident lorsque vous les modifiez ultérieurement. La configuration de base de l'environnement comprend

- Date et heure
- Locaux du système
- Disposition du clavier
- Langue

1.1. CONFIGURATION DE LA DATE ET DE L'HEURE

Un chronométrage précis est important pour plusieurs raisons. Dans Red Hat Enterprise Linux, la mesure du temps est assurée par le protocole **NTP**, qui est mis en œuvre par un démon s'exécutant dans l'espace utilisateur. Le démon de l'espace utilisateur met à jour l'horloge du système qui s'exécute dans le noyau. L'horloge système peut garder l'heure en utilisant différentes sources d'horloge.

Red Hat Enterprise Linux 9 et les versions ultérieures utilisent le démon **chronyd** pour implémenter **NTP**. **chronyd** est disponible à partir du paquetage **chrony** . Pour plus d'informations, voir Utilisation de la suite chrony pour configurer NTP.

1.1.1. Affichage de la date et de l'heure actuelles

Pour afficher la date et l'heure actuelles, procédez comme suit.

Procédure

1. Entrez la commande **date**:

```
$ date
Mon Mar 30 16:02:59 CEST 2020
```

2. Pour plus de détails, utilisez la commande **timedatectl**:

```
$ timedatectl
Local time: Mon 2020-03-30 16:04:42 CEST
Universal time: Mon 2020-03-30 14:04:42 UTC
  RTC time: Mon 2020-03-30 14:04:41
 Time zone: Europe/Prague (CEST, +0200)
System clock synchronized: yes
NTP service: active
RTC in local TZ: no
```

Ressources supplémentaires

- Configuration des paramètres horaires à l'aide de la console web
- **man date(1)** et **man timedatectl(1)**

1.2. CONFIGURATION DES PARAMÈTRES LINGUISTIQUES DU SYSTÈME

Les paramètres linguistiques du système sont stockés dans le fichier **/etc/locale.conf**, qui est lu au démarrage par le démon **systemd**. Chaque service ou utilisateur hérite des paramètres linguistiques configurés dans **/etc/locale.conf**, à moins que des programmes ou des utilisateurs individuels ne les remplacent.

Cette section décrit comment gérer les paramètres linguistiques du système.

Procédure

- Pour afficher la liste des paramètres régionaux disponibles :

```
$ localectl list-locales
C.utf8
aa_DJ
aa_DJ.iso88591
aa_DJ.utf8
...
```

- Pour afficher l'état actuel des paramètres locaux du système :

```
$ localectl status
```

- Pour définir ou modifier les paramètres linguistiques par défaut du système, utilisez la sous-commande **localectl set-locale** en tant qu'utilisateur **root**. Par exemple :

```
# localectl set-locale LANG=en_US
```

Ressources supplémentaires

- **man localectl(1)**, **man locale(7)**, et **man locale.conf(5)**

1.3. CONFIGURATION DE LA DISPOSITION DU CLAVIER

Les paramètres de disposition du clavier contrôlent la disposition utilisée dans la console de texte et les interfaces utilisateur graphiques.

Procédure

- Pour établir la liste des keymaps disponibles :

```
$ localectl list-keymaps
ANSI-dvorak
al
al-plisi
amiga-de
amiga-us
...
```

- Pour afficher l'état actuel des paramètres des cartes-clés :

```
$ localectl status
...
VC Keymap: us
...
```

- Pour définir ou modifier la cartographie des touches du système par défaut. Par exemple :

```
# localectl set-keymap us
```

Ressources supplémentaires

- **man localectl(1)**, **man locale(7)**, et **man locale.conf(5)**

1.4. CHANGER LA LANGUE À L'AIDE DE L'INTERFACE GRAPHIQUE DU BUREAU

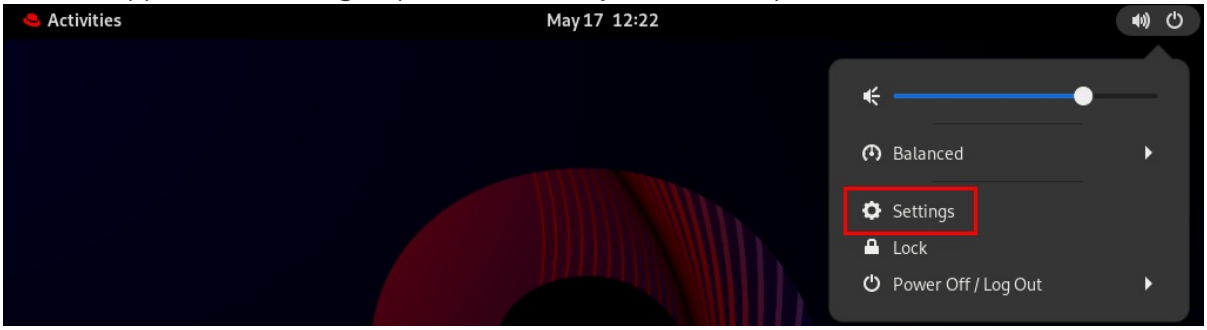
Cette section décrit comment changer la langue du système à l'aide de l'interface graphique du bureau.

Conditions préalables

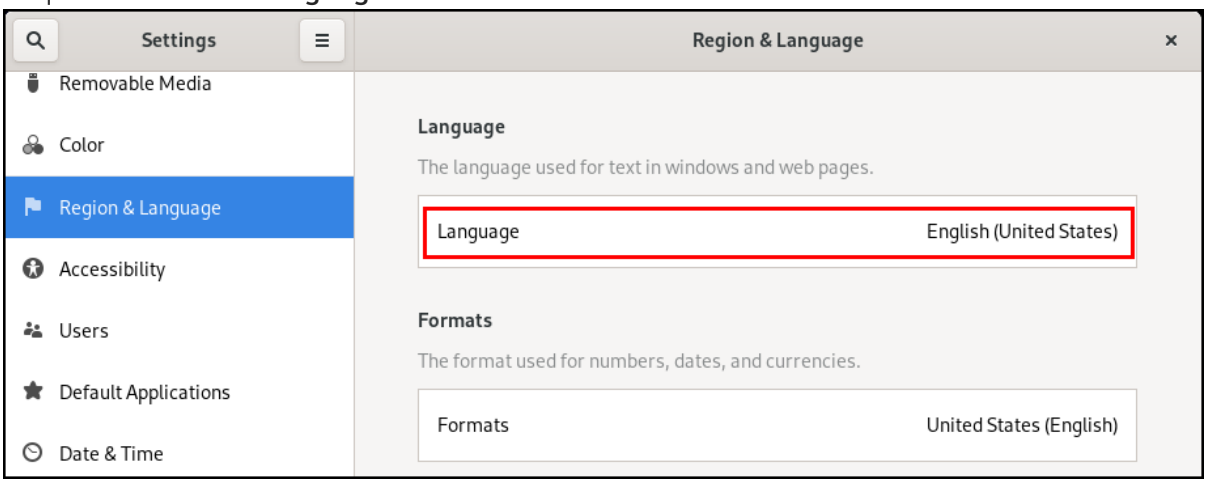
- Les paquets linguistiques requis sont installés sur votre système

Procédure

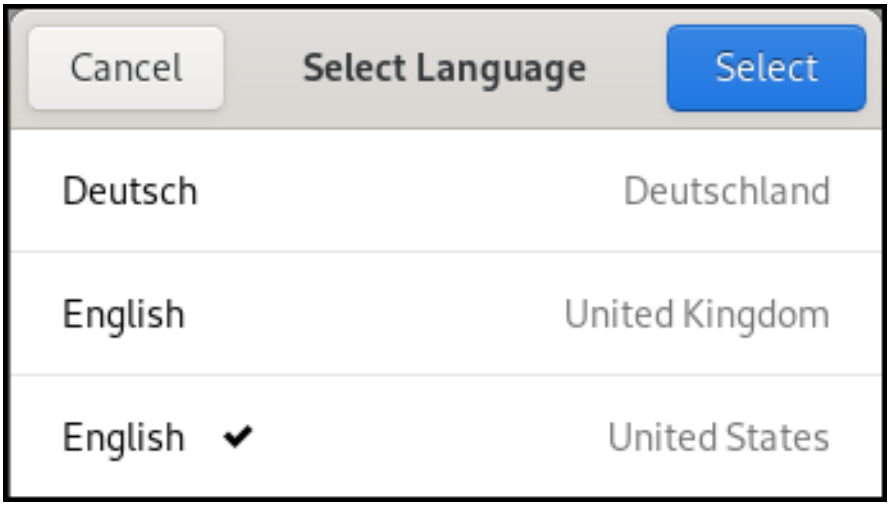
1. Ouvrez l'application **Settings** à partir du menu système en cliquant sur son icône.



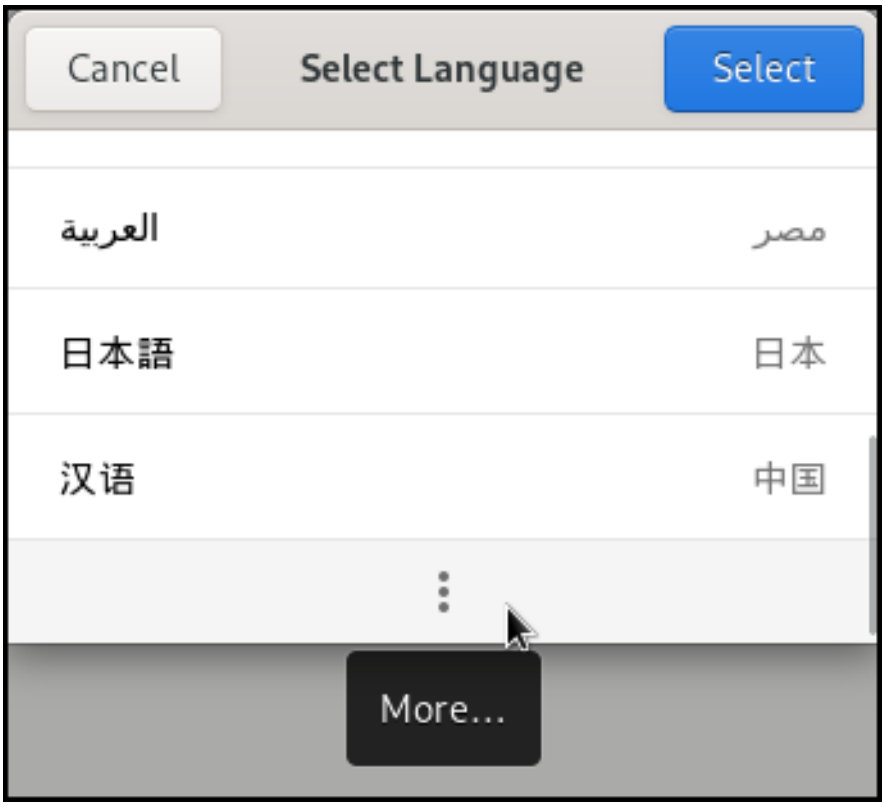
2. Dans **Settings**, choisissez **Region & Language** dans la barre latérale gauche.
3. Cliquez sur le menu **Language**.



4. Sélectionnez la région et la langue souhaitées dans le menu.

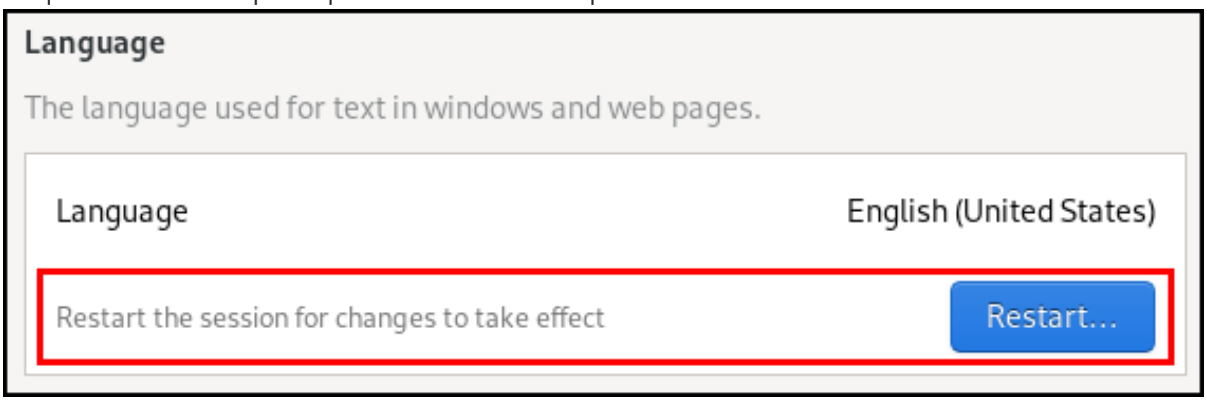


Si votre région et votre langue ne figurent pas dans la liste, faites défiler vers le bas et cliquez sur **More** pour sélectionner l'une des régions et l'une des langues disponibles.



5. Cliquez sur **Done**.

6. Cliquez sur **Restart** pour que les modifications prennent effet.



NOTE

Certaines applications ne prennent pas en charge certaines langues. Le texte d'une application qui ne peut être traduit dans la langue sélectionnée reste en anglais américain.

Ressources supplémentaires

- Lancement d'applications dans GNOME

1.5. RESSOURCES SUPPLÉMENTAIRES

- Effectuer une installation standard de RHEL 9

CHAPITRE 2. INTRODUCTION AUX RÔLES DU SYSTÈME RHEL

Vous pouvez automatiser l'administration du système sur plusieurs systèmes avec RHEL System Roles.

RHEL System Roles est une collection de rôles et de modules Ansible. En utilisant RHEL System Roles, vous pouvez gérer à distance les configurations système de plusieurs systèmes RHEL dans les principales versions de RHEL. Pour l'utiliser afin de configurer des systèmes, vous devez utiliser les composants suivants :

Nœud de contrôle

Un nœud de contrôle est le système à partir duquel vous exécutez les commandes et les playbooks Ansible. Votre nœud de contrôle peut être une Ansible Automation Platform, Red Hat Satellite ou un hôte RHEL 9, 8 ou 7. Pour plus d'informations, voir Préparation d'un nœud de contrôle sur RHEL 9 .

Nœud géré

Les nœuds gérés sont les serveurs et les périphériques réseau que vous gérez avec Ansible. Les nœuds gérés sont aussi parfois appelés hôtes. Il n'est pas nécessaire d'installer Ansible sur les nœuds gérés. Pour plus d'informations, voir Préparation d'un nœud géré .

Playbook Ansible

Dans un cahier de jeu, vous définissez la configuration que vous souhaitez obtenir sur vos nœuds gérés ou un ensemble d'étapes à exécuter par le système sur le nœud géré. Les playbooks sont le langage de configuration, de déploiement et d'orchestration d'Ansible.

Inventaire

Dans un fichier d'inventaire, vous dressez la liste des nœuds gérés et spécifiez des informations telles que l'adresse IP de chaque nœud géré. Dans l'inventaire, vous pouvez également organiser les nœuds gérés en créant et en imbriquant des groupes pour faciliter la mise à l'échelle. Un fichier d'inventaire est aussi parfois appelé fichier d'hôte.

Sur Red Hat Enterprise Linux 9, vous pouvez utiliser les rôles suivants fournis par le paquetage **rhel-system-roles**, qui est disponible dans le référentiel **AppStream**:

Nom du rôle	Description du rôle	Titre du chapitre
certificate	Délivrance et renouvellement du certificat	Demande de certificats à l'aide des rôles système RHEL
cockpit	Console web	Installation et configuration de la console web avec le cockpit RHEL System Role
crypto_policies	Politiques cryptographiques à l'échelle du système	Définition d'une politique cryptographique personnalisée pour l'ensemble des systèmes
firewall	Firewalld	Configuration de firewalld à l'aide des rôles système
ha_cluster	Cluster HA	Configuration d'un cluster à haute disponibilité à l'aide des rôles système

Nom du rôle	Description du rôle	Titre du chapitre
kdump	Fiches du noyau	Configuration de kdump à l'aide des rôles système RHEL
kernel_settings	Paramètres du noyau	Utiliser les rôles Ansible pour configurer de façon permanente les paramètres du noyau
logging	Enregistrement	Utilisation du rôle de système de journalisation
metrics	Métriques (PCP)	Surveillance des performances à l'aide des rôles système RHEL
network	Mise en réseau	Utilisation du rôle de système RHEL de réseau pour gérer les connexions InfiniBand
nbde_client	Client Network Bound Disk Encryption	Utilisation des rôles système nbde_client et nbde_server
nbde_server	Serveur de cryptage de disque lié au réseau	Utilisation des rôles système nbde_client et nbde_server
postfix	Postfixe	Variables du rôle postfixe dans Rôles du système
selinux	SELinux	Configuration de SELinux à l'aide des rôles système
ssh	Client SSH	Configuration de la communication sécurisée avec les rôles du système ssh
sshd	Serveur SSH	Configuration de la communication sécurisée avec les rôles du système ssh
storage	Stockage	Gestion du stockage local à l'aide des rôles système RHEL
tlog	Enregistrement de la session du terminal	Configuration d'un système pour l'enregistrement de sessions à l'aide du rôle de système RHEL tlog

Nom du rôle	Description du rôle	Titre du chapitre
timesync	Synchronisation du temps	Configuration de la synchronisation temporelle à l'aide des rôles système RHEL
vpn	VPN	Configurer des connexions VPN avec IPsec en utilisant le rôle système RHEL vpn

Ressources supplémentaires

- Automatiser l'administration du système en utilisant les rôles système RHEL
- Rôles du système Red Hat Enterprise Linux (RHEL)
- **/usr/share/doc/rhel-system-roles/** fournie par le paquet **rhel-system-roles**

CHAPITRE 3. CONFIGURATION ET GESTION DE L'ACCÈS AU RÉSEAU

Cette section décrit les différentes options permettant d'ajouter des connexions Ethernet dans Red Hat Enterprise Linux.

3.1. CONFIGURATION DU RÉSEAU ET DU NOM D'HÔTE EN MODE D'INSTALLATION GRAPHIQUE

Suivez les étapes de cette procédure pour configurer votre réseau et votre nom d'hôte.

Procédure

1. Dans la fenêtre **Installation Summary**, cliquez sur **Réseau et nom d'hôte**.
2. Dans la liste du volet de gauche, sélectionnez une interface. Les détails s'affichent dans le volet de droite.

NOTE

- Il existe plusieurs types de normes de dénomination des périphériques réseau utilisées pour identifier les périphériques réseau avec des noms persistants, par exemple, **em1** et **wl3sp0**. Pour plus d'informations sur ces normes, voir le *Configuring and managing networking* document.

3. Basculer l'interrupteur **ON**/**OFF** pour activer ou désactiver l'interface sélectionnée.

NOTE

Le programme d'installation détecte automatiquement les interfaces accessibles localement et vous ne pouvez pas les ajouter ou les supprimer manuellement.

4. Cliquez sur pour ajouter une interface réseau virtuelle, qui peut être soit : Team (obsolète), Bond, Bridge ou VLAN.
5. Cliquez sur **-** pour supprimer une interface virtuelle.
6. Cliquez sur **Configurer** pour modifier les paramètres tels que les adresses IP, les serveurs DNS ou la configuration du routage pour une interface existante (virtuelle et physique).
7. Saisissez le nom d'hôte de votre système dans le champ **Host Name**.

NOTE

- Le nom d'hôte peut être un nom de domaine entièrement qualifié (FQDN) au format ***hostname.domainname***ou un nom d'hôte court sans le domaine. De nombreux réseaux disposent d'un service DHCP (Dynamic Host Configuration Protocol) qui attribue automatiquement un nom de domaine aux systèmes connectés. Pour permettre au service DHCP d'attribuer le nom de domaine à ce système, indiquez uniquement le nom d'hôte abrégé.

- Lors de l'utilisation de l'IP statique et de la configuration du nom d'hôte, l'utilisation d'un nom court ou d'un FQDN dépend du cas d'utilisation du système prévu. Red Hat Identity Management configure le FQDN pendant le provisionnement, mais certains logiciels tiers peuvent exiger un nom court. Dans les deux cas, pour garantir la disponibilité des deux formes dans toutes les situations, ajoutez une entrée pour l'hôte dans **/etc/hosts**` au format **IP FQDN short-alias**.

- La valeur **localhost** signifie qu'aucun nom d'hôte statique spécifique n'est configuré pour le système cible et que le nom d'hôte réel du système installé est configuré pendant le traitement de la configuration du réseau, par exemple par NetworkManager à l'aide de DHCP ou de DNS.

- Les noms d'hôtes ne peuvent contenir que des caractères alphanumériques et **-** ou **.**. Le nom d'hôte doit être inférieur ou égal à 64 caractères. Les noms d'hôtes ne peuvent pas commencer ou se terminer par **-** et **.**. Pour être conforme au DNS, chaque partie d'un FQDN doit être inférieure ou égale à 63 caractères et la longueur totale du FQDN, y compris les points, ne doit pas dépasser 255 caractères.

8. Cliquez sur **Appliquer** pour appliquer le nom d'hôte à l'environnement d'installation.

9. Vous pouvez également choisir l'option Sans fil dans la fenêtre **Network and Hostname**. Cliquez sur **Sélectionner un réseau** dans le volet de droite pour sélectionner votre connexion wifi, entrez le mot de passe si nécessaire et cliquez sur **Terminé**.

Ressources supplémentaires

- Effectuer une installation avancée de RHEL 9

3.2. CONFIGURATION D'UNE CONNEXION ETHERNET AVEC UNE ADRESSE IP STATIQUE À L'AIDE DE NMCLI

Pour configurer une connexion Ethernet sur la ligne de commande, utilisez l'utilitaire **nmcli**.

Par exemple, la procédure ci-dessous crée un profil de connexion NetworkManager pour le périphérique **enp7s0** avec les paramètres suivants :

- Une adresse IPv4 statique - **192.0.2.1** avec un masque de sous-réseau **/24**
- Une adresse IPv6 statique - **2001:db8:1::1** avec un masque de sous-réseau **/64**
- Une passerelle par défaut IPv4 - **192.0.2.254**
- Une passerelle par défaut IPv6 - **2001:db8:1::fffe**

- Un serveur DNS IPv4 - **192.0.2.200**
- Un serveur DNS IPv6 - **2001:db8:1::ffbb**
- Un domaine de recherche DNS - **example.com**

Conditions préalables

- Un périphérique Ethernet physique ou virtuel existe dans la configuration du serveur.

Procédure

1. Ajouter un nouveau profil de connexion NetworkManager pour la connexion Ethernet :

```
# nmcli connection add con-name Example-Connection ifname enp7s0 type ethernet
```

   Les étapes suivantes modifient le profil de connexion **Example-Connection** que vous avez créé.

2. Définir l'adresse IPv4 :

```
# nmcli connection modify Example-Connection ipv4.addresses 192.0.2.1/24
```

3. Définir l'adresse IPv6 :

```
# nmcli connection modify Example-Connection ipv6.addresses 2001:db8:1::1/64
```

4. Réglez la méthode de connexion IPv4 et IPv6 sur **manual**:

```
# nmcli connection modify Example-Connection ipv4.method manual
# nmcli connection modify Example-Connection ipv6.method manual
```

5. Définir les passerelles par défaut IPv4 et IPv6 :

```
# nmcli connection modify Example-Connection ipv4.gateway 192.0.2.254
# nmcli connection modify Example-Connection ipv6.gateway 2001:db8:1::fffe
```

6. Définissez les adresses des serveurs DNS IPv4 et IPv6 :

```
# nmcli connection modify Example-Connection ipv4.dns "192.0.2.200"
# nmcli connection modify Example-Connection ipv6.dns "2001:db8:1::ffbb"
```

   Pour définir plusieurs serveurs DNS, indiquez-les en les séparant par des espaces et en les plaçant entre guillemets.

7. Définir le domaine de recherche DNS pour la connexion IPv4 et IPv6 :

```
# nmcli connection modify Example-Connection ipv4.dns-search example.com
# nmcli connection modify Example-Connection ipv6.dns-search example.com
```

8. Activer le profil de connexion :

```
# nmcli connection up Example-Connection
Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/13)
```

Vérification

1. Affiche l'état des appareils et des connexions :

```
# nmcli device status
DEVICE      TYPE      STATE      CONNECTION
enp7s0      ethernet  connected  Example-Connection
```

2. Utilisez l'utilitaire **ping** pour vérifier que cet hôte peut envoyer des paquets à d'autres hôtes :

```
# ping host_name_or_IP_address
```

Résolution de problèmes

- Vérifiez que le câble réseau est branché sur l'hôte et sur un commutateur.
- Vérifiez si la défaillance de la liaison existe uniquement sur cet hôte ou également sur d'autres hôtes connectés au même commutateur.
- Vérifiez que le câble réseau et l'interface réseau fonctionnent comme prévu. Effectuez les étapes de diagnostic du matériel et remplacez les câbles et les cartes d'interface réseau défectueux.
- Si la configuration du disque ne correspond pas à celle du périphérique, le démarrage ou le redémarrage de NetworkManager crée une connexion en mémoire qui reflète la configuration du périphérique. Pour plus de détails et pour savoir comment éviter ce problème, voir NetworkManager duplique une connexion après le redémarrage du service NetworkManager .

Ressources supplémentaires

- **nm-settings(5)** page de manuel
- **nmcli(1)** page de manuel
- Configurer NetworkManager pour éviter d'utiliser un profil spécifique pour fournir une passerelle par défaut

3.3. CONFIGURATION D'UNE CONNEXION ETHERNET AVEC UNE ADRESSE IP DYNAMIQUE À L'AIDE DE NMTUI

L'application **nmtui** fournit une interface utilisateur textuelle pour NetworkManager. Vous pouvez utiliser **nmtui** pour configurer une connexion Ethernet avec une adresse IP dynamique sur un hôte sans interface graphique.

NOTE

Sur **nmtui**:

- Naviguer à l'aide des touches du curseur.
- Appuyez sur un bouton en le sélectionnant et en appuyant sur **Entrée**.
- Sélectionnez et désélectionnez les cases à cocher en utilisant l'**espace**.

Conditions préalables

- Un périphérique Ethernet physique ou virtuel existe dans la configuration du serveur.
- Un serveur DHCP est disponible dans le réseau.

Procédure

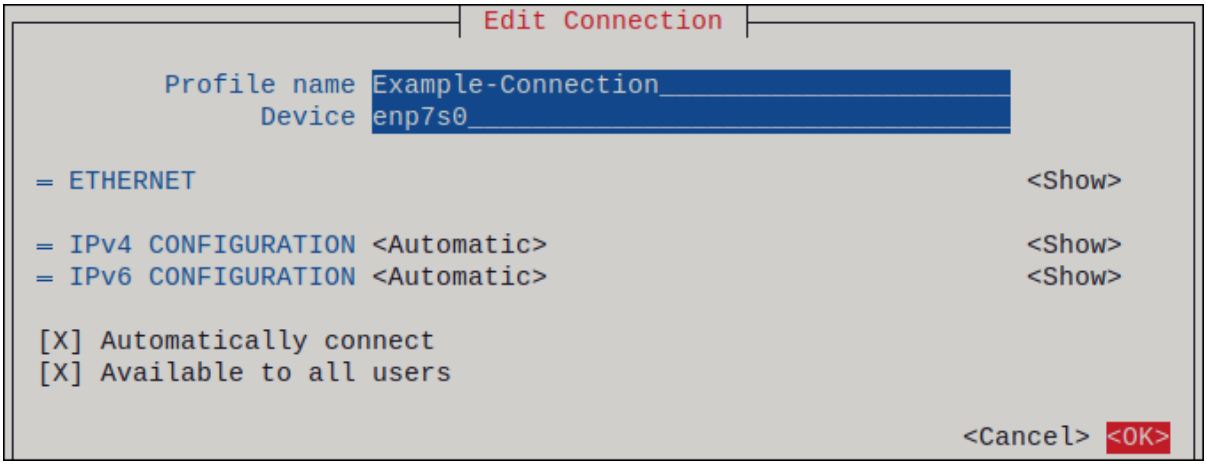
1. Si vous ne connaissez pas le nom du périphérique réseau que vous souhaitez utiliser pour la connexion, affichez les périphériques disponibles :

```
# nmcli device status
DEVICE     TYPE      STATE                CONNECTION
enp7s0     ethernet  unavailable          --
...
```

2. Démarrer **nmtui**:

```
# nmtui
```

3. Sélectionnez **Edit a connection** et appuyez sur **Enter**.
4. Appuyez sur le bouton **Add**.
5. Sélectionnez **Ethernet** dans la liste des types de réseaux et appuyez sur **Entrée**.
6. Optionnel : Entrez un nom pour le profil NetworkManager à créer.
7. Saisissez le nom de l'appareil réseau dans le champ **Device**.
8. Appuyez sur le bouton **OK** pour créer et activer automatiquement la nouvelle connexion.



9. Appuyez sur le bouton **Back** pour revenir au menu principal.

10. Sélectionnez **Quit** et appuyez sur **Entrée** pour fermer l'application **nmtui**.

Vérification

1. Affiche l'état des appareils et des connexions :

```
# nmcli device status
DEVICE     TYPE      STATE      CONNECTION
enp7s0     ethernet  connected  Example-Connection
```

2. Utilisez l'utilitaire **ping** pour vérifier que cet hôte peut envoyer des paquets à d'autres hôtes :

```
# ping host_name_or_IP_address
```

Résolution de problèmes

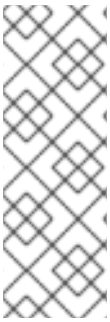
- Vérifiez que le câble réseau est branché sur l'hôte et sur un commutateur.
- Vérifiez si la défaillance de la liaison existe uniquement sur cet hôte ou également sur d'autres hôtes connectés au même commutateur.
- Vérifiez que le câble réseau et l'interface réseau fonctionnent comme prévu. Effectuez les étapes de diagnostic du matériel et remplacez les câbles et les cartes d'interface réseau défectueux.
- Si la configuration du disque ne correspond pas à celle du périphérique, le démarrage ou le redémarrage de NetworkManager crée une connexion en mémoire qui reflète la configuration du périphérique. Pour plus de détails et pour savoir comment éviter ce problème, voir NetworkManager duplique une connexion après le redémarrage du service NetworkManager .

Ressources supplémentaires

- Configurer NetworkManager pour éviter d'utiliser un profil spécifique pour fournir une passerelle par défaut

3.4. CONFIGURATION D'UNE CONNEXION ETHERNET AVEC UNE ADRESSE IP STATIQUE À L'AIDE DE NMTUI

L'application **nmtui** fournit une interface utilisateur textuelle pour NetworkManager. Vous pouvez utiliser **nmtui** pour configurer une connexion Ethernet avec une adresse IP statique sur un hôte sans interface graphique.



NOTE

Sur **nmtui**:

- Naviguer à l'aide des touches du curseur.
- Appuyez sur un bouton en le sélectionnant et en appuyant sur **Entrée**.
- Sélectionnez et désélectionnez les cases à cocher en utilisant l'**espace**.

Conditions préalables

- Un périphérique Ethernet physique ou virtuel existe dans la configuration du serveur.

Procédure

1. Si vous ne connaissez pas le nom du périphérique réseau que vous souhaitez utiliser pour la connexion, affichez les périphériques disponibles :

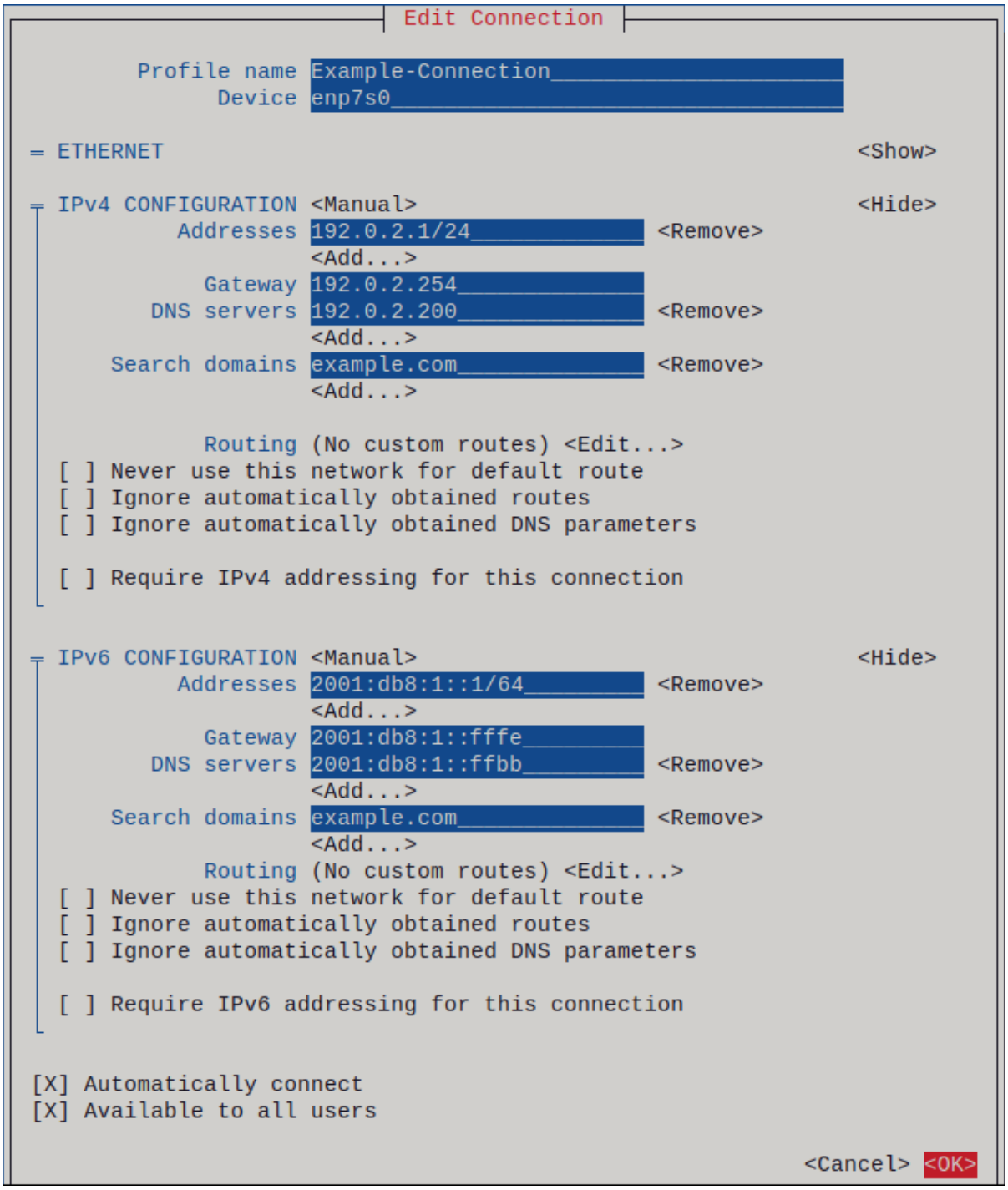
```
# nmcli device status
DEVICE     TYPE      STATE                CONNECTION
enp7s0     ethernet  unavailable          --
...
```

2. Démarrer **nmtui**:

```
# nmtui
```

3. Sélectionnez **Edit a connection** et appuyez sur **Enter**.
4. Appuyez sur le bouton **Add**.
5. Sélectionnez **Ethernet** dans la liste des types de réseaux et appuyez sur **Entrée**.
6. Optionnel : Entrez un nom pour le profil NetworkManager à créer.
7. Saisissez le nom de l'appareil réseau dans le champ **Device**.
8. Configurez les paramètres des adresses IPv4 et IPv6 dans les zones **IPv4 configuration** et **IPv6 configuration**:
   a. Appuyez sur la touche **Automatic** et sélectionnez **Manual** dans la liste affichée.
   b. Appuyez sur le bouton **Show** en regard du protocole que vous souhaitez configurer pour afficher des champs supplémentaires.
   c. Appuyez sur le bouton **Add** à côté de **Addresses**, et entrez l'adresse IP et le masque de sous-réseau au format CIDR (Classless Inter-Domain Routing).
   Si vous ne spécifiez pas de masque de sous-réseau, NetworkManager définit un masque de sous-réseau /**32** pour les adresses IPv4 et /**64** pour les adresses IPv6.
   d. Saisissez l'adresse de la passerelle par défaut.
   e. Appuyez sur la touche **Add** à côté de **DNS servers**, et entrez l'adresse du serveur DNS.
   f. Appuyez sur la touche **Add** à côté de **Search domains**, et entrez le domaine de recherche DNS.

Figure 3.1. Exemple d'une connexion Ethernet avec des paramètres d'adresse IP statiques



9. Appuyez sur le bouton **OK** pour créer et activer automatiquement la nouvelle connexion.
10. Appuyez sur le bouton **Back** pour revenir au menu principal.
11. Sélectionnez **Quit** et appuyez sur **Entrée** pour fermer l'application **nmtui**.

Vérification

1. Affiche l'état des appareils et des connexions :

```
# nmcli device status
DEVICE     TYPE      STATE      CONNECTION
enp7s0     ethernet  connected  Example-Connection
```

2. Utilisez l'utilitaire **ping** pour vérifier que cet hôte peut envoyer des paquets à d'autres hôtes :

```
# ping host_name_or_IP_address
```

Résolution de problèmes

- Vérifiez que le câble réseau est branché sur l'hôte et sur un commutateur.
- Vérifiez si la défaillance de la liaison existe uniquement sur cet hôte ou également sur d'autres hôtes connectés au même commutateur.
- Vérifiez que le câble réseau et l'interface réseau fonctionnent comme prévu. Effectuez les étapes de diagnostic du matériel et remplacez les câbles et les cartes d'interface réseau défectueux.
- Si la configuration du disque ne correspond pas à celle du périphérique, le démarrage ou le redémarrage de NetworkManager crée une connexion en mémoire qui reflète la configuration du périphérique. Pour plus de détails et pour savoir comment éviter ce problème, voir NetworkManager duplique une connexion après le redémarrage du service NetworkManager .

Ressources supplémentaires

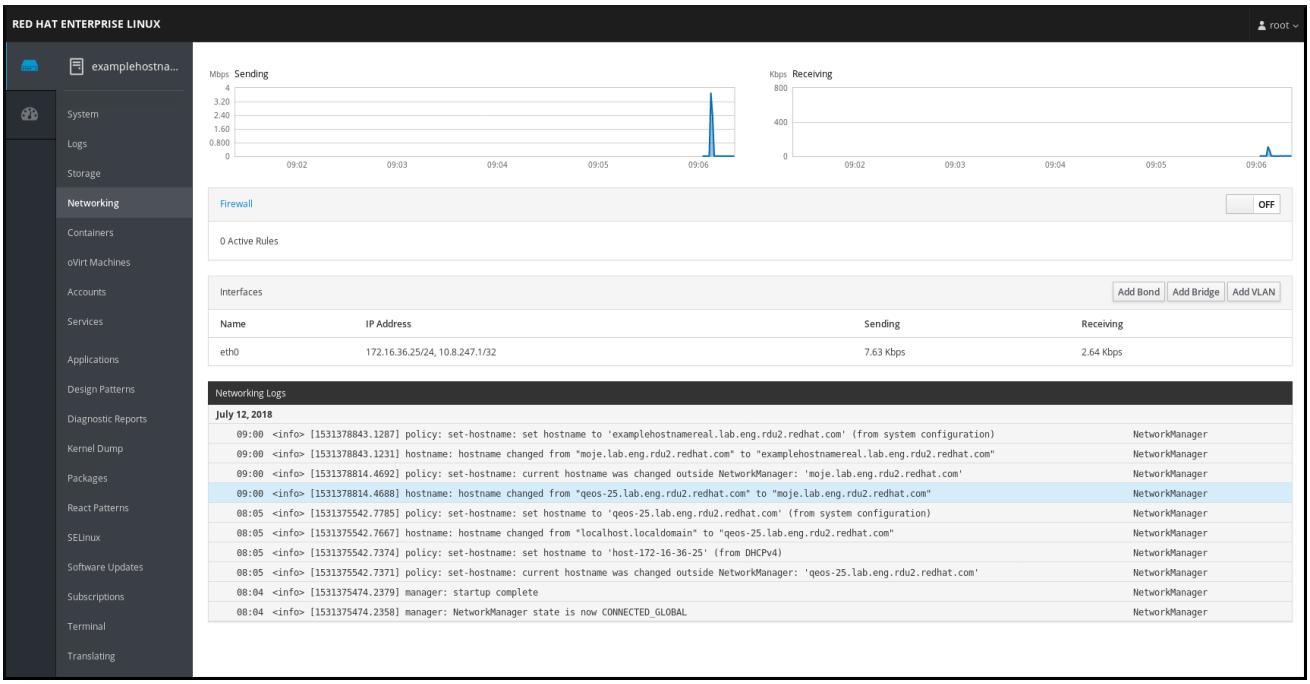
- Configurer NetworkManager pour éviter d'utiliser un profil spécifique pour fournir une passerelle par défaut

3.5. GESTION DE LA MISE EN RÉSEAU DANS LA CONSOLE WEB RHEL

Dans la console web, le menu **Réseau** vous permet :

- Pour afficher les paquets actuellement reçus et envoyés
- Pour afficher les principales caractéristiques des interfaces réseau disponibles
- Pour afficher le contenu des journaux de réseau.
- Pour ajouter différents types d'interfaces réseau (bond, team, bridge, VLAN)

Figure 3.2. Gestion de la mise en réseau dans la console web RHEL



3.6. GESTION DE LA MISE EN RÉSEAU À L'AIDE DES RÔLES SYSTÈME RHEL

Vous pouvez configurer les connexions réseau sur plusieurs machines cibles à l'aide du rôle **network**.

Le rôle **network** permet de configurer les types d'interfaces suivants :

- Ethernet
- Pont
- Collé
- VLAN
- MacVLAN
- InfiniBand

Les connexions réseau requises pour chaque hôte sont fournies sous forme de liste dans la variable **network_connections**.

AVERTISSEMENT

Le rôle **network** met à jour ou crée tous les profils de connexion sur le système cible exactement comme spécifié dans la variable **network_connections**. Par conséquent, le rôle **network** supprime les options des profils spécifiés si les options ne sont présentes que sur le système mais pas dans la variable **network_connections**.

L'exemple suivant montre comment appliquer le rôle **network** pour s'assurer qu'il existe une connexion Ethernet avec les paramètres requis :

Un exemple de playbook appliquant le rôle de réseau pour établir une connexion Ethernet avec les paramètres requis

```
# SPDX-License-Identifier: BSD-3-Clause
---
- hosts: managed-node-01.example.com
  vars:
    network_connections:

      # Create one Ethernet profile and activate it.
      # The profile uses automatic IP addressing
      # and is tied to the interface by MAC address.
      - name: prod1
        state: up
        type: ethernet
        autoconnect: yes
        mac: "00:00:5e:00:53:00"
        mtu: 1450

  roles:
    - rhel-system-roles.network
```

Ressources supplémentaires

- Préparation d'un nœud de contrôle et de nœuds gérés à l'utilisation des rôles système RHEL

3.7. RESSOURCES SUPPLÉMENTAIRES

- Configuring and managing networking

CHAPITRE 4. ENREGISTREMENT DU SYSTÈME ET GESTION DES ABONNEMENTS

Les abonnements couvrent les produits installés sur Red Hat Enterprise Linux, y compris le système d'exploitation lui-même.

Vous pouvez utiliser un abonnement à Red Hat Content Delivery Network pour assurer le suivi :

- Systèmes enregistrés
- Produits installés sur vos systèmes
- Abonnements attachés aux produits installés

4.1. ENREGISTREMENT DU SYSTÈME APRÈS L'INSTALLATION

Utilisez la procédure suivante pour enregistrer votre système si vous ne l'avez pas déjà enregistré au cours de la procédure d'installation.

Conditions préalables

- Un compte utilisateur valide dans le portail client de Red Hat.
- Consultez la page Créer un login Red Hat .
- Un abonnement actif pour le système RHEL.
- Pour plus d'informations sur le processus d'installation, voir Effectuer une installation standard de RHEL 9.

Procédure

1. Enregistrez et abonnez automatiquement votre système en une seule étape :

```
# subscription-manager register --username <username> --password <password> --auto-attach
Registering to: subscription.rhsm.redhat.com:443/subscription
The system has been registered with ID: 37to907c-ece6-49ea-9174-20b87ajk9ee7
The registered system name is: client1.idm.example.com
Installed Product Current Status:
Product Name: Red Hat Enterprise Linux for x86_64
Status:       Subscribed
```

La commande vous invite à saisir votre nom d'utilisateur et votre mot de passe du portail client Red Hat.

Si la procédure d'enregistrement échoue, vous pouvez enregistrer votre système auprès d'un pool spécifique. Pour savoir comment procéder, suivez les étapes suivantes :

a. Déterminez l'ID du pool d'un abonnement dont vous avez besoin :

```
# subscription-manager list --available
```

Cette commande affiche tous les abonnements disponibles pour votre compte Red Hat. Pour chaque abonnement, diverses caractéristiques sont affichées, y compris l'ID du pool.

b. Attachez l'abonnement approprié à votre système en remplaçant *pool_id* par l'ID du pool déterminé à l'étape précédente :

```
# subscription-manager attach --pool=pool_id
```

NOTE

Pour enregistrer le système avec Red Hat Insights, vous pouvez utiliser l'utilitaire **rhc connect**. Reportez-vous à Configuration de l'hôte distant .

Ressources supplémentaires

- Comprendre le rattachement automatique des abonnements sur le portail client
- Comprendre l'enregistrement manuel et l'inscription sur le portail client

4.2. ENREGISTRER DES ABONNEMENTS AVEC DES INFORMATIONS D'IDENTIFICATION DANS LA CONSOLE WEB

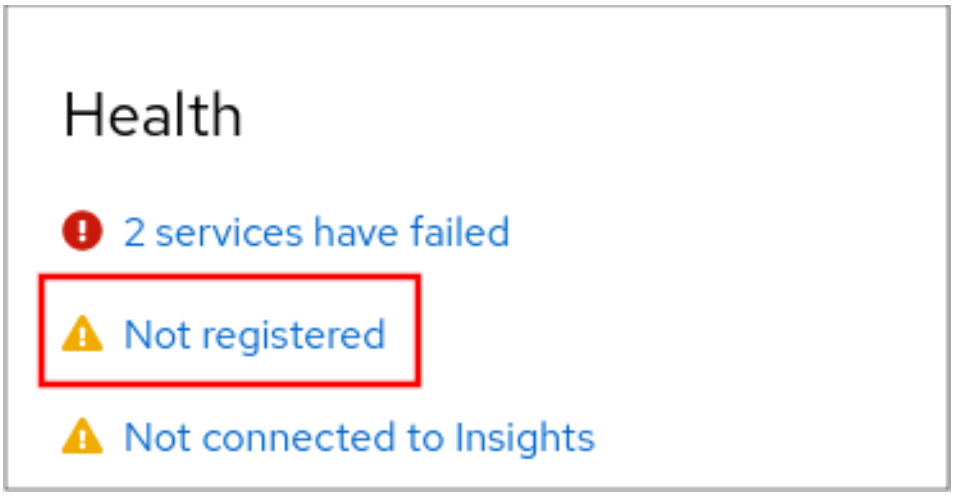
Suivez les étapes suivantes pour enregistrer un Red Hat Enterprise Linux nouvellement installé avec les informations d'identification du compte à l'aide de la console Web RHEL.

Conditions préalables

- Un compte utilisateur valide sur le portail client de Red Hat.
  Consultez la page Créer un login Red Hat .
- Abonnement actif pour votre système RHEL.

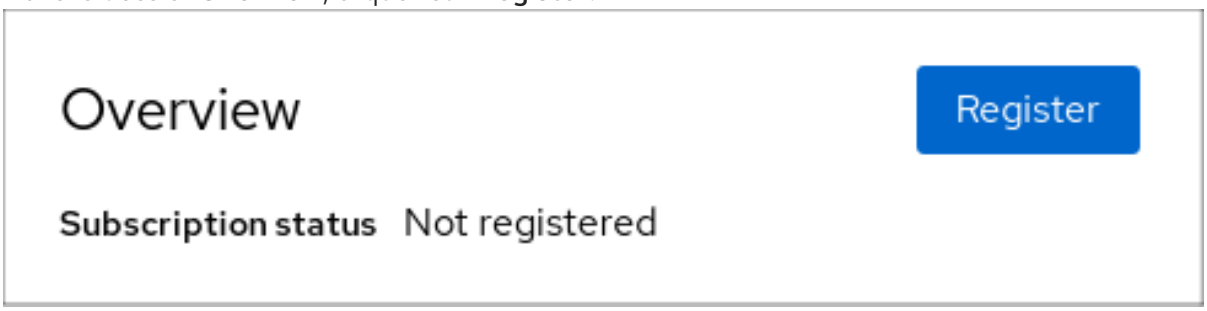
Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Dans le dossier **Health** de la page **Overview**, cliquez sur l'avertissement **Not registered**, ou cliquez sur **Subscriptions** dans le menu principal pour accéder à la page contenant vos informations d'abonnement.

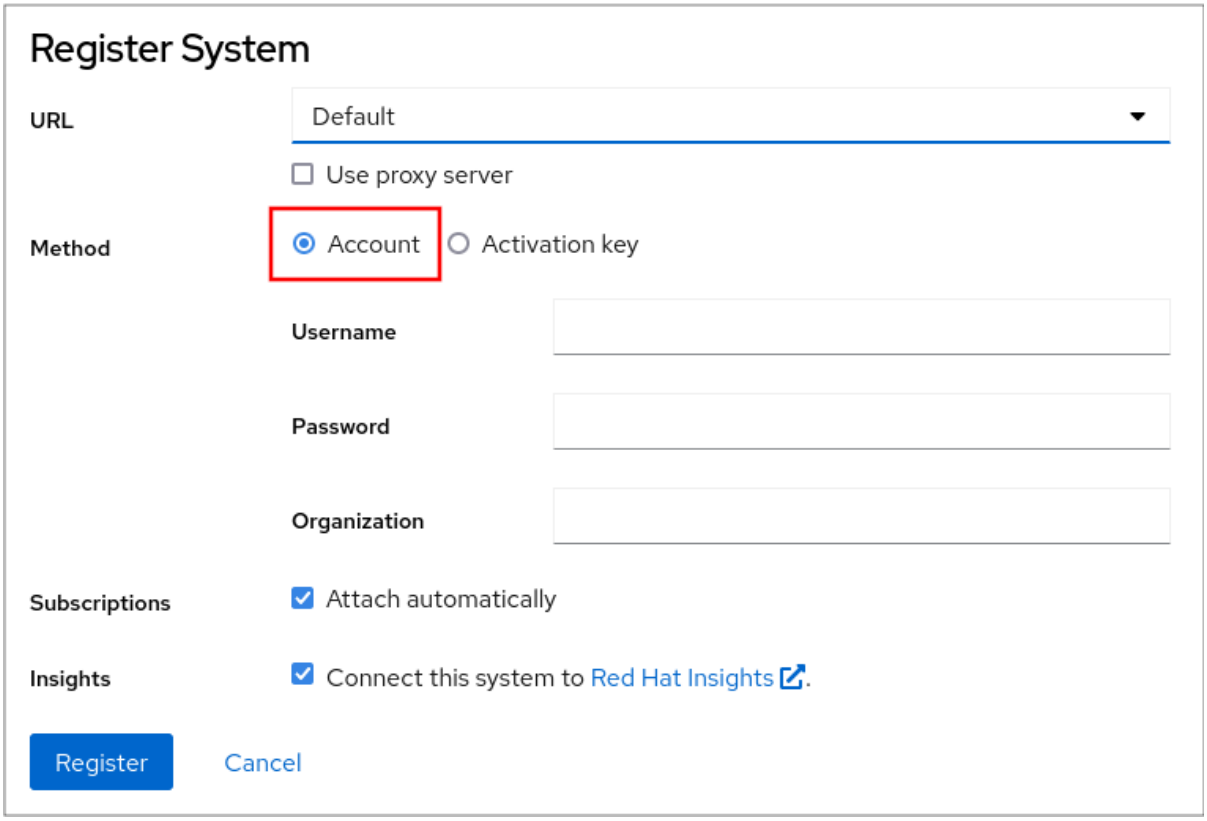


.

3. Dans le dossier **Overview**, cliquez sur **Register**.



4. Dans la boîte de dialogue **Register system**, indiquez que vous souhaitez vous enregistrer en utilisant les informations d'identification de votre compte.



5. Entrez votre nom d'utilisateur.

6. Entrez votre mot de passe.

7. Si vous le souhaitez, vous pouvez saisir le nom ou l'identifiant de votre organisation.
Si votre compte appartient à plus d'une organisation sur le portail client de Red Hat, vous devez ajouter le nom de l'organisation ou l'ID de l'organisation. Pour obtenir l'identifiant de l'organisation, adressez-vous à votre point de contact Red Hat.

   - Si vous ne souhaitez pas connecter votre système à Red Hat Insights, décochez la case **Insights**.

8. Cliquez sur le bouton **Enregistrer**.

À ce stade, votre système Red Hat Enterprise Linux a été enregistré avec succès.

4.3. ENREGISTREMENT D'UN SYSTÈME À L'AIDE DU COMPTE RED HAT SUR GNOME

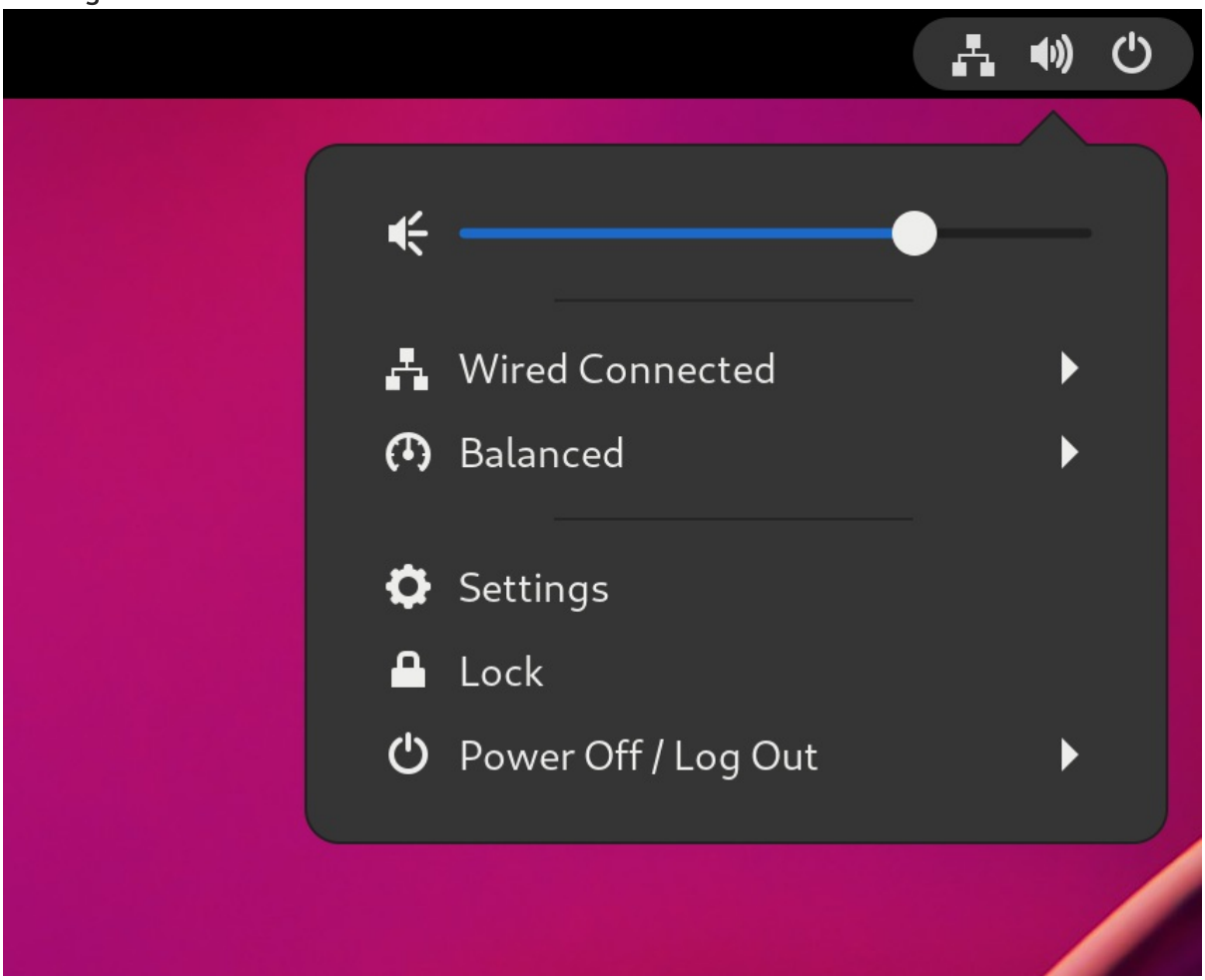
Suivez les étapes de cette procédure pour inscrire votre système avec votre compte Red Hat.

Conditions préalables

- Un compte valide sur le portail client de Red Hat.
  Consultez la page Créer un login Red Hat pour l'enregistrement d'un nouvel utilisateur.

Procédure

1. Ouvrez le site **system menu**, accessible dans le coin supérieur droit de l'écran, et cliquez sur **Settings**.



2. Aller à **A propos de → Abonnement**.
3. Si vous n'utilisez pas le serveur Red Hat :
   a. Dans la section **Registration Server**, sélectionnez **Custom Address**.
   b. Entrez l'adresse du serveur dans le champ **URL**.
4. Dans la section **Registration Type**, sélectionnez **Red Hat Account**
5. Dans la section **Registration Details**:
   - Saisissez le nom d'utilisateur de votre compte Red Hat dans le champ **Login**.
   - Saisissez le mot de passe de votre compte Red Hat dans le champ **Password**.
   - Saisissez le nom de votre organisation dans le champ **Organization**.

6. Cliquez sur **Enregistrer**.

4.4. ENREGISTRER UN SYSTÈME À L'AIDE D'UNE CLÉ D'ACTIVATION SUR GNOME

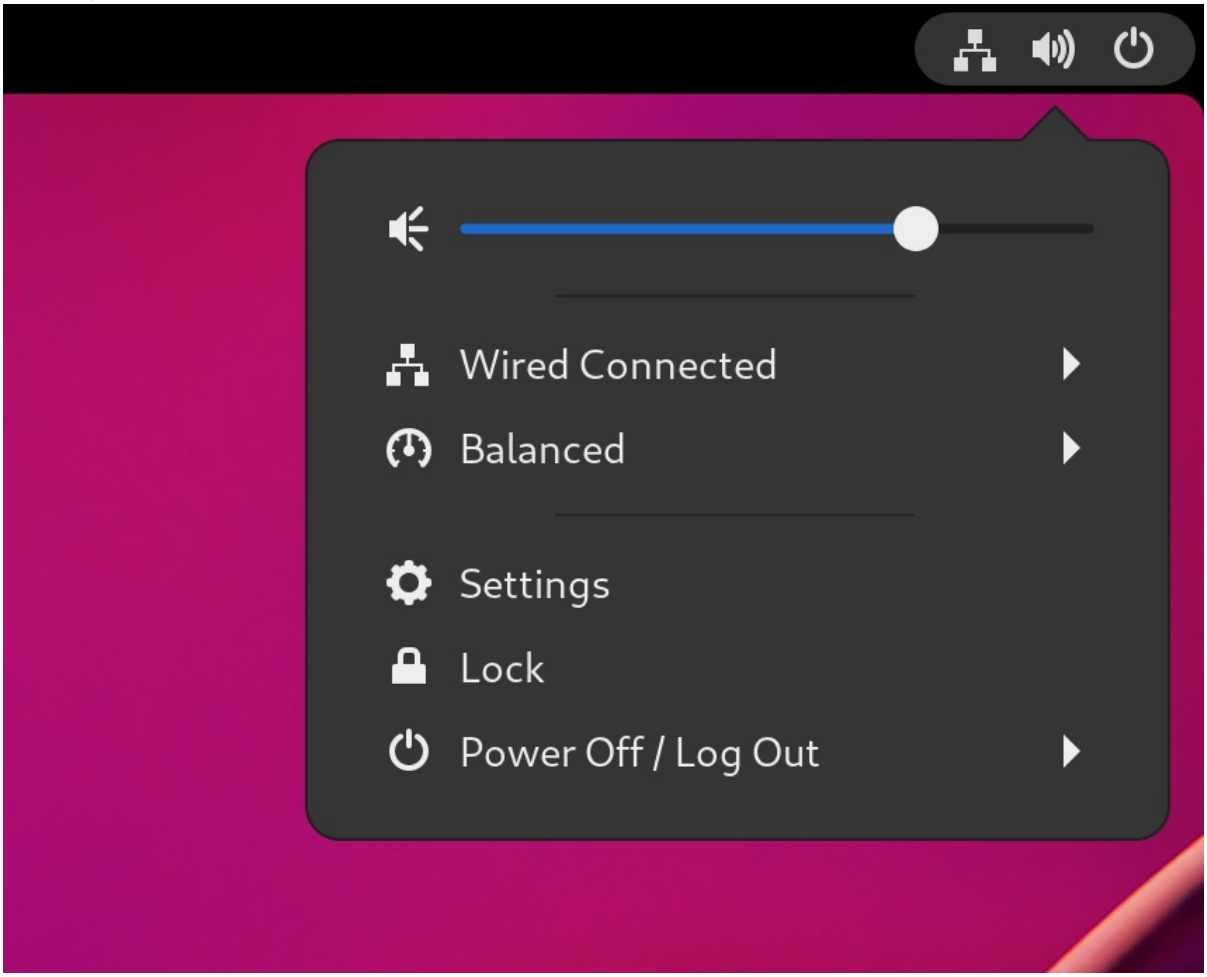
Suivez les étapes de cette procédure pour enregistrer votre système avec une clé d'activation. Vous pouvez obtenir la clé d'activation auprès de l'administrateur de votre organisation.

Conditions préalables

- Clé(s) d'activation.
  Voir la page Clés d'activation pour créer de nouvelles clés d'activation.

Procédure

1. Ouvrez le site **system menu**, accessible dans le coin supérieur droit de l'écran, et cliquez sur **Settings**.



2. Aller à **A propos de** → **Abonnement**.
3. Si vous n'utilisez pas le serveur Red Hat :
   a. Dans la section **Registration Server**, sélectionnez **Custom Address**.
   b. Entrez l'adresse du serveur dans le champ **URL**.
4. Dans la section **Registration Type**, sélectionnez **Activation Keys**.

5. Sous **Registration Details**:
    - Saisissez vos clés d'activation dans le champ **Activation Keys**.
      Séparez vos clés par une virgule (**,**).
    - Saisissez le nom ou l'identifiant de votre organisation dans le champ **Organization**.
6. Cliquez sur **Enregistrer**.

CHAPITRE 5. CONFIGURATION DE LA SÉCURITÉ DU SYSTÈME

La sécurité informatique est la protection des systèmes informatiques et de leur matériel, des logiciels, des informations et des services contre le vol, les dommages, les perturbations et les erreurs d'aiguillage. Assurer la sécurité informatique est une tâche essentielle, en particulier dans les entreprises qui traitent des données sensibles et effectuent des transactions commerciales.

Cette section ne couvre que les fonctions de sécurité de base que vous pouvez configurer après l'installation du système d'exploitation.

5.1. ACTIVATION DU SERVICE FIREWALLD

Un pare-feu est un système de sécurité réseau qui surveille et contrôle le trafic réseau entrant et sortant selon des règles de sécurité configurées. Un pare-feu établit généralement une barrière entre un réseau interne sécurisé et fiable et un autre réseau extérieur.

Le service **firewalld**, qui fournit un pare-feu dans Red Hat Enterprise Linux, est automatiquement activé lors de l'installation.

Pour activer le service **firewalld**, suivez cette procédure.

Procédure

- Afficher l'état actuel de **firewalld**:

```
$ systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset:
enabled)
   Active: inactive (dead)
...
```

- Si **firewalld** n'est pas activé et ne fonctionne pas, passez à l'utilisateur **root**, démarrez le service **firewalld** et activez-le pour qu'il démarre automatiquement après le redémarrage du système :

```
# systemctl enable --now firewalld
```

Verification steps

- Vérifiez que **firewalld** fonctionne et est activé :

```
$ systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset:
enabled)
   Active: active (running)
...
```

Ressources supplémentaires

- Utilisation et configuration de firewalld
- **man firewalld(1)**

5.2. GESTION DES PARAMÈTRES SELINUX DE BASE

Security-Enhanced Linux (SELinux) est une couche supplémentaire de sécurité du système qui détermine quels processus peuvent accéder à quels fichiers, répertoires et ports. Ces autorisations sont définies dans les règles SELinux. Une politique est un ensemble de règles qui guident le moteur de sécurité SELinux.

SELinux a deux états possibles :

- Handicapés
- Activé

Lorsque SELinux est activé, il fonctionne dans l'un des modes suivants :

- Activé
  - Mise en œuvre
  - Permissif

Dans **enforcing mode**, SELinux applique les politiques chargées. SELinux refuse l'accès sur la base des règles de la politique SELinux et n'autorise que les interactions qui sont explicitement autorisées. Le mode "Enforcing" est le mode SELinux le plus sûr et le mode par défaut après l'installation.

Dans **permissive mode**, SELinux n'applique pas les politiques chargées. SELinux ne refuse pas l'accès, mais signale les actions qui enfreignent les règles dans le journal **/var/log/audit/audit.log**. Le mode permissif est le mode par défaut lors de l'installation. Le mode permissif est également utile dans certains cas spécifiques, par exemple lors de la résolution de problèmes.

Ressources supplémentaires

- Utilisation de SELinux

5.3. ASSURER L'ÉTAT REQUIS DE SELINUX

Par défaut, SELinux fonctionne en mode "enforcing". Toutefois, dans certains cas, il est possible de passer en mode permissif, voire de désactiver SELinux.

IMPORTANT

Red Hat recommande de garder votre système en mode "enforcing". À des fins de débogage, vous pouvez configurer SELinux en mode permissif.

Suivez cette procédure pour modifier l'état et le mode de SELinux sur votre système.

Procédure

1. Affiche le mode SELinux actuel :

```
$ getenforce
```

2. Pour activer temporairement SELinux :
   a. Passer en mode "Enforcing" :

```
# setenforce Enforcing
```

b. Vers le mode permissif :

```
# setenforce Permissive
```

NOTE

Après le redémarrage, le mode SELinux prend la valeur spécifiée dans le fichier de configuration **/etc/selinux/config**.

3. Pour que le mode SELinux persiste après les redémarrages, modifiez la variable **SELINUX** dans le fichier de configuration **/etc/selinux/config**.
Par exemple, pour faire passer SELinux en mode d'application :

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
...
```

AVERTISSEMENT

La désactivation de SELinux réduit la sécurité de votre système. Évitez de désactiver SELinux à l'aide de l'option **SELINUX=disabled** du fichier **/etc/selinux/config**, car cela peut entraîner des fuites de mémoire et des conditions de course provoquant des paniques du noyau. Désactivez plutôt SELinux en ajoutant le paramètre **selinux=0** à la ligne de commande du noyau. Pour plus d'informations, voir Modifier les modes SELinux au démarrage.

Ressources supplémentaires

- Modifier les états et les modes SELinux

5.4. RESSOURCES SUPPLÉMENTAIRES

- Générer des paires de clés SSH
- Configuration d'un serveur OpenSSH pour l'authentification par clé
- Renforcement de la sécurité
- Utilisation de SELinux
- Sécurisation des réseaux

CHAPITRE 6. COMMENCER À GÉRER LES COMPTES D'UTILISATEURS

Red Hat Enterprise Linux est un système d'exploitation multi-utilisateurs, qui permet à plusieurs utilisateurs sur différents ordinateurs d'accéder à un système unique installé sur une machine. Chaque utilisateur fonctionne avec son propre compte, et la gestion des comptes d'utilisateurs représente donc un élément central de l'administration du système Red Hat Enterprise Linux.

Les différents types de comptes d'utilisateurs sont décrits ci-dessous :

- **Normal user accounts:**
  Les comptes normaux sont créés pour les utilisateurs d'un système particulier. Ces comptes peuvent être ajoutés, supprimés et modifiés au cours de l'administration normale du système.

- **System user accounts:**
  Les comptes d'utilisateurs du système représentent un identifiant d'application particulier sur un système. Ces comptes ne sont généralement ajoutés ou manipulés qu'au moment de l'installation du logiciel et ne sont pas modifiés par la suite.

  AVERTISSEMENT

  Les comptes système sont supposés être disponibles localement sur un système. Si ces comptes sont configurés et fournis à distance, comme dans le cas d'une configuration LDAP, des pannes du système et des échecs de démarrage de service peuvent se produire.

  Pour les comptes système, les identifiants inférieurs à 1000 sont réservés. Pour les comptes normaux, vous pouvez utiliser des identifiants à partir de 1000. Toutefois, il est recommandé d'attribuer des identifiants à partir de 5000. Pour l'attribution des identifiants, voir le fichier **/etc/login.defs**.

- **Group:**
  Un groupe est une entité qui relie plusieurs comptes d'utilisateurs dans un but commun, par exemple pour accorder l'accès à des fichiers particuliers.

6.1. GESTION DES COMPTES ET DES GROUPES À L'AIDE D'OUTILS DE LIGNE DE COMMANDE

Cette section décrit les outils de base de la ligne de commande pour gérer les comptes et les groupes d'utilisateurs.

- Pour afficher les ID des utilisateurs et des groupes :

```
$ id
uid=1000(example.user) gid=1000(example.user) groups=1000(example.user),10(wheel)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

- Pour créer un nouveau compte utilisateur :

```
# useradd example.user
```

- Pour attribuer un nouveau mot de passe à un compte d'utilisateur appartenant à *example.user*:

```
# passwd example.user
```

- Pour ajouter un utilisateur à un groupe :

```
# usermod -a -G example.group example.user
```

Ressources supplémentaires

- **man useradd(8)**, **man passwd(1)**, et **man usermod(8)**

6.2. COMPTES D'UTILISATEURS DU SYSTÈME GÉRÉS DANS LA CONSOLE WEB

Avec les comptes d'utilisateurs affichés dans la console web RHEL, vous pouvez :

- Authentifier les utilisateurs lors de l'accès au système.
- Définir les droits d'accès au système.

La console web RHEL affiche tous les comptes d'utilisateurs situés dans le système. Par conséquent, vous pouvez voir au moins un compte d'utilisateur juste après la première connexion à la console web.

Après vous être connecté à la console web RHEL, vous pouvez effectuer les opérations suivantes :

- Créer de nouveaux comptes utilisateurs.
- Modifier leurs paramètres.
- Verrouiller les comptes.
- Mettre fin aux sessions des utilisateurs.

6.3. AJOUTER DE NOUVEAUX COMPTES À L'AIDE DE LA CONSOLE WEB

Les étapes suivantes permettent d'ajouter des comptes d'utilisateurs au système et de définir des droits d'administration pour les comptes via la console web RHEL.

Conditions préalables

- La console web RHEL doit être installée et accessible. Pour plus de détails, voir Installation de la console web.

Procédure

1. Connectez-vous à la console web RHEL.
2. Cliquez sur **Comptes**.

3. Cliquez sur **Créer un nouveau compte**.

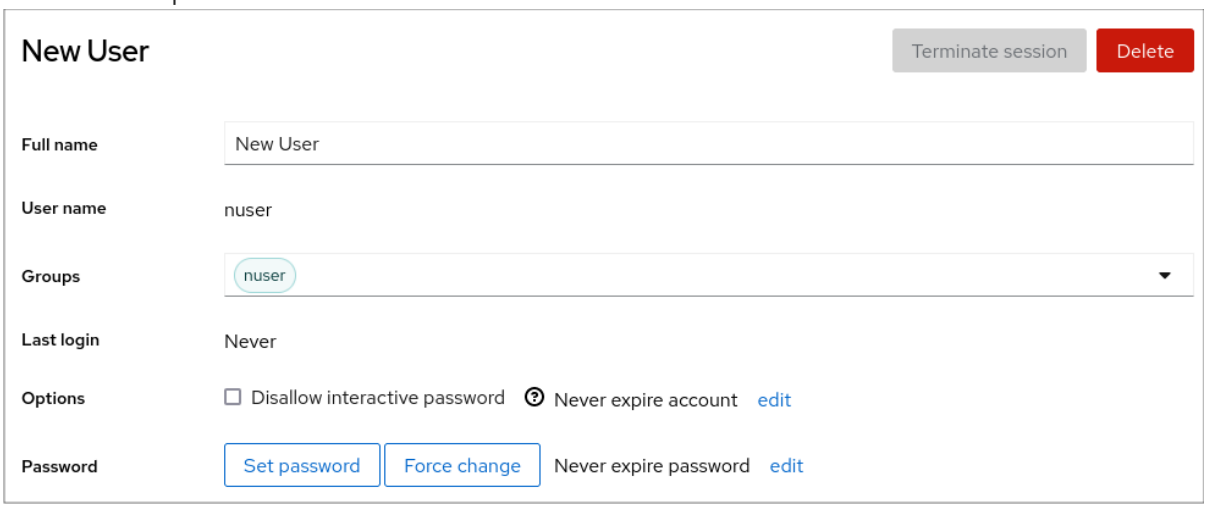
4. Dans le champ **Full Name**, saisissez le nom complet de l'utilisateur.
   La console web RHEL suggère automatiquement un nom d'utilisateur à partir du nom complet et le remplit dans le champ **User Name**. Si vous ne souhaitez pas utiliser la convention de dénomination originale qui consiste à utiliser la première lettre du prénom et le nom de famille complet, mettez à jour la suggestion.

5. Dans les champs **Password/Confirm**, saisissez le mot de passe et retapez-le pour vérifier qu'il est correct.
   La barre de couleur située sous les champs indique le niveau de sécurité du mot de passe saisi, ce qui ne permet pas de créer un utilisateur avec un mot de passe faible.

6. Cliquez sur **Créer** pour enregistrer les paramètres et fermer la boîte de dialogue.

7. Sélectionnez le compte nouvellement créé.

8. Dans le menu déroulant **Groups**, sélectionnez les groupes que vous souhaitez ajouter au nouveau compte.



Vous pouvez maintenant voir le nouveau compte dans les paramètres de **Accounts** et vous pouvez utiliser ses informations d'identification pour vous connecter au système.

CHAPITRE 7. VIDAGE D'UN NOYAU ACCIDENTÉ POUR ANALYSE ULTÉRIEURE

Pour analyser la raison pour laquelle un système est tombé en panne, vous pouvez utiliser le service **kdump** pour sauvegarder le contenu de la mémoire du système en vue d'une analyse ultérieure. Cette section présente brièvement **kdump** et fournit des informations sur la configuration de **kdump** à l'aide de la console Web RHEL ou du rôle système RHEL correspondant.

7.1. QU'EST-CE QUE KDUMP ?

kdump est un service qui fournit un mécanisme de vidage en cas de panne. Ce service vous permet de sauvegarder le contenu de la mémoire du système à des fins d'analyse. **kdump** utilise l'appel système **kexec** pour démarrer dans le second noyau (a *capture kernel*) sans redémarrer ; il capture ensuite le contenu de la mémoire du noyau accidenté (a *crash dump* ou a *vmcore*) et l'enregistre dans un fichier. Le second noyau réside dans une partie réservée de la mémoire du système.

IMPORTANT

Un crash dump du noyau peut être la seule information disponible en cas de défaillance du système (bogue critique). Par conséquent, le site opérationnel **kdump** est important dans les environnements critiques. Red Hat conseille aux administrateurs système de mettre à jour et de tester régulièrement **kexec-tools** dans le cadre du cycle normal de mise à jour du noyau. Ceci est particulièrement important lorsque de nouvelles fonctionnalités du noyau sont mises en œuvre.

Vous pouvez activer **kdump** pour tous les noyaux installés sur une machine ou seulement pour des noyaux spécifiques. Cette option est utile lorsque plusieurs noyaux sont utilisés sur une machine, dont certains sont suffisamment stables pour ne pas risquer de tomber en panne.

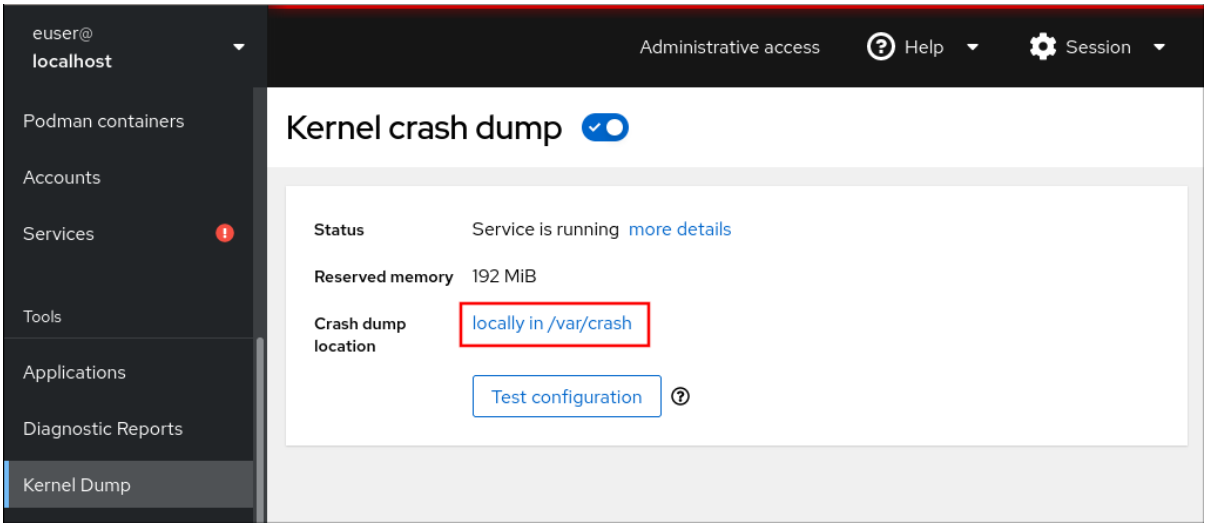
Lors de l'installation de **kdump**, un fichier par défaut **/etc/kdump.conf** est créé. Ce fichier contient la configuration minimale par défaut de **kdump**. Vous pouvez modifier ce fichier pour personnaliser la configuration de **kdump**, mais ce n'est pas obligatoire.

7.2. CONFIGURER L'UTILISATION DE LA MÉMOIRE DE KDUMP ET L'EMPLACEMENT DE LA CIBLE DANS LA CONSOLE WEB

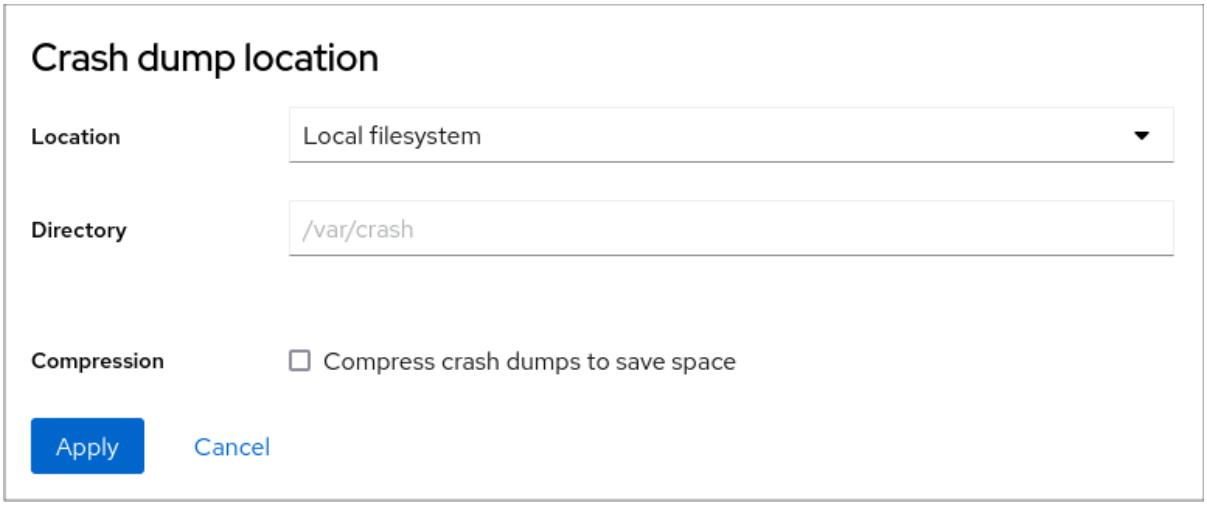
La procédure ci-dessous vous montre comment utiliser l'onglet **Kernel Dump** dans l'interface de la console web RHEL pour configurer la quantité de mémoire réservée au noyau **kdump**. La procédure décrit également comment spécifier l'emplacement cible du fichier dump **vmcore** et comment tester votre configuration.

Procédure

1. Ouvrez l'onglet **Kernel Dump** et démarrez le service **kdump**.
2. Configurez l'utilisation de la mémoire de **kdump** à l'aide de la ligne de commande.
3. Cliquez sur le lien situé à côté de l'option **Crash dump location**.



4. Sélectionnez l'option **Local Filesystem** dans le menu déroulant et indiquez le répertoire dans lequel vous souhaitez enregistrer le dump.



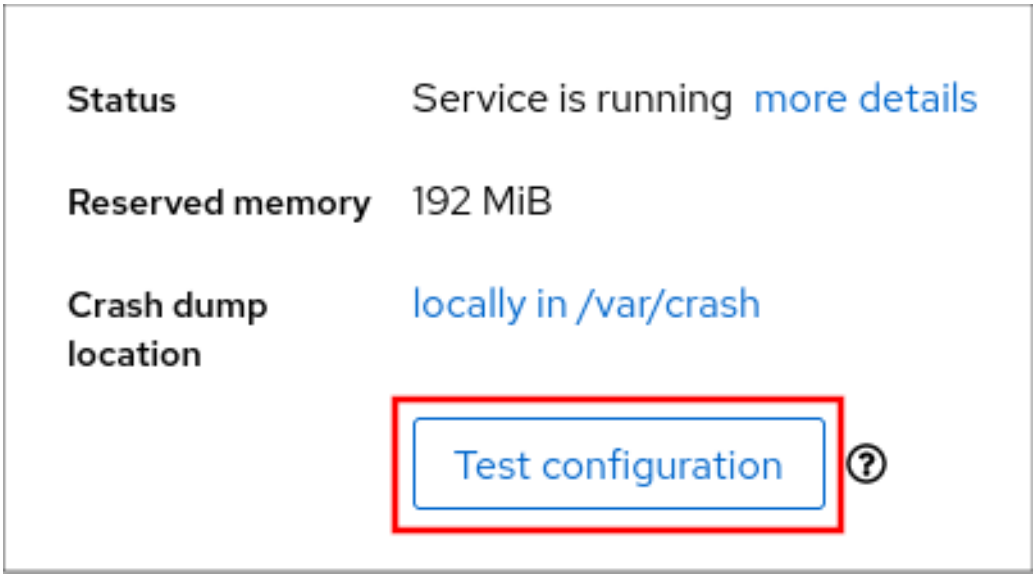
- Vous pouvez également sélectionner l'option **Remote over SSH** dans le menu déroulant pour envoyer le vmcore à une machine distante à l'aide du protocole SSH.
  Remplissez les champs **Server**, **ssh key**, et **Directory** avec l'adresse de la machine distante, l'emplacement de la clé ssh et un répertoire cible.

- Une autre possibilité consiste à sélectionner l'option **Remote over NFS** dans la liste déroulante et à remplir le champ **Mount** pour envoyer le noyau virtuel à une machine distante à l'aide du protocole NFS.

NOTE

Cochez la case **Compression** pour réduire la taille du fichier vmcore.

5. Testez votre configuration en plantant le noyau.



a. Cliquez sur **Test configuration**.

b. Dans le champ **Test kdump settings**, cliquez sur **Crash system**.

> **AVERTISSEMENT**
>
> Cette étape perturbe l'exécution du noyau et entraîne une panne du système et une perte de données.

Ressources supplémentaires

- Cibles kdump prises en charge
- Utiliser des communications sécurisées entre deux systèmes avec OpenSSH

7.3. KDUMP À L'AIDE DES RÔLES SYSTÈME RHEL

RHEL System Roles est une collection de rôles et de modules Ansible qui fournissent une interface de configuration cohérente pour gérer à distance plusieurs systèmes RHEL. Le rôle **kdump** vous permet de définir des paramètres de vidage de noyau de base sur plusieurs systèmes.

> **AVERTISSEMENT**
>
> Le rôle **kdump** remplace entièrement la configuration **kdump** des hôtes gérés en remplaçant le fichier **/etc/kdump.conf**. De plus, si le rôle **kdump** est appliqué, tous les paramètres précédents de **kdump** sont également remplacés, même s'ils ne sont pas spécifiés par les variables de rôle, en remplaçant le fichier **/etc/sysconfig/kdump**.

L'exemple suivant montre comment appliquer le rôle système **kdump** pour définir l'emplacement des fichiers de vidage en cas de panne :

```
---
- hosts: kdump-test
  vars:
    kdump_path: /var/crash
  roles:
    - rhel-system-roles.kdump
```

Pour une référence détaillée sur les variables de rôle **kdump**, installez le paquetage **rhel-system-roles** et consultez les fichiers **README.md** ou **README.html** dans le répertoire **/usr/share/doc/rhel-system-roles/kdump**.

Ressources supplémentaires

- Introduction aux rôles du système RHEL

7.4. RESSOURCES SUPPLÉMENTAIRES

- Installation de kdump
- Configuration de kdump sur la ligne de commande
- Configuration de kdump dans la console web

CHAPITRE 8. RÉCUPÉRATION ET RESTAURATION D'UN SYSTÈME

Pour récupérer et restaurer un système à l'aide d'une sauvegarde existante, Red Hat Enterprise Linux fournit l'utilitaire Relax-and-Recover (ReaR).

Vous pouvez utiliser l'utilitaire comme solution de reprise après sinistre et pour la migration du système.

L'utilitaire vous permet d'effectuer les tâches suivantes :

- Produire une image de démarrage et restaurer le système à partir d'une sauvegarde existante, en utilisant l'image.
- Reproduire le schéma de stockage d'origine.
- Restaurer les fichiers de l'utilisateur et du système.
- Restaurer le système sur un autre matériel.

En outre, pour la reprise après sinistre, vous pouvez également intégrer certains logiciels de sauvegarde à ReaR.

La mise en place de ReaR implique les étapes de haut niveau suivantes :

1. Installer ReaR.
2. Modifier le fichier de configuration de ReaR, pour ajouter les détails de la méthode de sauvegarde.
3. Créer un système de secours.
4. Générer des fichiers de sauvegarde.

8.1. MISE EN PLACE DE REAR

Les étapes suivantes permettent d'installer le paquetage pour l'utilisation de l'utilitaire Relax-and-Recover (ReaR), de créer un système de secours, de configurer et de générer une sauvegarde.

Conditions préalables

- Les configurations nécessaires selon le plan de restauration de la sauvegarde sont prêtes. Notez que vous pouvez utiliser la méthode de sauvegarde **NETFS**, une méthode entièrement intégrée à ReaR.

Procédure

1. Installez l'utilitaire ReaR en exécutant la commande suivante :

```
# dnf install rear
```

2. Modifiez le fichier de configuration de ReaR dans un éditeur de votre choix, par exemple :

```
# vi /etc/rear/local.conf
```

3. Ajoutez les détails de la configuration de la sauvegarde à **/etc/rear/local.conf**. Par exemple, dans le cas de la méthode de sauvegarde **NETFS**, ajoutez les lignes suivantes :

```
BACKUP=NETFS
BACKUP_URL=backup.location
```

   Remplacez *backup.location* par l'URL de votre emplacement de sauvegarde.

4. Pour configurer ReaR afin qu'il conserve l'archive de sauvegarde précédente lors de la création de la nouvelle, ajoutez également la ligne suivante au fichier de configuration :

```
NETFS_KEEP_OLD_BACKUP_COPY=y
```

5. Pour que les sauvegardes soient incrémentielles, c'est-à-dire que seuls les fichiers modifiés sont sauvegardés à chaque exécution, ajoutez la ligne suivante :

```
BACKUP_TYPE=incremental
```

6. Créer un système de secours :

```
# rear mkrescue
```

7. Effectuez une sauvegarde conformément au plan de restauration. Par exemple, dans le cas de la méthode de sauvegarde **NETFS**, exécutez la commande suivante :

```
# rear mkbackuponly
```

   Vous pouvez également créer le système de secours et la sauvegarde en une seule étape en exécutant la commande suivante :

```
# rear mkbackup
```

   Cette commande combine les fonctionnalités des commandes **rear mkrescue** et **rear mkbackuponly**.

8.2. UTILISATION D'UNE IMAGE DE SECOURS REAR SUR L'ARCHITECTURE IBM Z 64 BITS

La fonctionnalité de base Relax and Recover (ReaR) est désormais disponible sur l'architecture IBM Z 64 bits en tant qu'aperçu technologique. Vous pouvez créer une image de secours ReaR sur IBM Z uniquement dans l'environnement z/VM. La sauvegarde et la récupération des partitions logiques (LPAR) n'ont pas été testées.

IMPORTANT

ReaR sur l'architecture IBM Z 64 bits n'est pris en charge qu'avec le paquetage **rear** version 2.6-17.el9 ou ultérieure. Les versions antérieures ne sont disponibles qu'en tant que fonctionnalité d'aperçu technologique. Pour plus d'informations sur l'étendue de la prise en charge des fonctionnalités Technology Preview de Red Hat, consultez https://access.redhat.com/support/offerings/techpreview.

La seule méthode de sortie actuellement disponible est le chargement de programme initial (IPL). L'IPL produit un noyau et un disque RAM initial (initrd) qui peut être utilisé avec le chargeur de démarrage **zIPL**.

Conditions préalables

- ReaR est installé.
  - Pour installer ReaR, exécutez la commande **dnf install rear**

Procédure

Ajoutez les variables suivantes au site **/etc/rear/local.conf** pour configurer ReaR afin de produire une image de secours sur l'architecture IBM Z 64 bits :

1. Pour configurer la méthode de sortie **IPL**, ajoutez **OUTPUT=IPL**.
2. Pour configurer la méthode de sauvegarde et la destination, ajoutez les variables **BACKUP** et **BACKUP_URL**. Par exemple :

```
BACKUP=NETFS

BACKUP_URL=nfs://<nfsserver name>/<share path>
```

IMPORTANT

Le stockage local de sauvegarde n'est actuellement pas pris en charge sur l'architecture IBM Z 64 bits.

3. En option, vous pouvez également configurer la variable **OUTPUT_URL** pour enregistrer les fichiers kernel et **initrd**. Par défaut, le fichier **OUTPUT_URL** est aligné avec **BACKUP_URL**.
4. Pour effectuer une sauvegarde et créer une image de secours :

```
rear mkbackup
```

5. Cette opération crée les fichiers kernel et initrd à l'emplacement spécifié par la variable **BACKUP_URL** ou **OUTPUT_URL** (si elle est définie), ainsi qu'une sauvegarde à l'aide de la méthode de sauvegarde spécifiée.
6. Pour récupérer le système, utilisez les fichiers ReaR kernel et initrd créés à l'étape 3 et démarrez à partir d'un DASD (Direct Attached Storage Device) ou d'un périphérique SCSI relié au protocole Fibre Channel (FCP) préparé avec le chargeur de démarrage **zipl**, le kernel et **initrd**. Pour plus d'informations, voir Utilisation d'un DASD préparé .
7. Lorsque le noyau de secours et **initrd** sont démarrés, l'environnement de secours ReaR est lancé. Procédez à la récupération du système.

AVERTISSEMENT

Actuellement, le processus de récupération reformate tous les DASD (Direct Attached Storage Devices) connectés au système. Ne tentez pas de récupérer le système si des données de valeur sont présentes sur les périphériques de stockage du système. Cela inclut également le périphérique préparé avec le chargeur de démarrage zipl, le noyau ReaR et l'initrd qui ont été utilisés pour démarrer dans l'environnement de secours. Veillez à en conserver une copie.

Ressources supplémentaires

- Installation sous z/VM
- Utilisation d'un DASD préparé

CHAPITRE 9. RÉSOLUTION DES PROBLÈMES À L'AIDE DES FICHIERS JOURNAUX

Les fichiers journaux contiennent des messages sur le système, y compris le noyau, les services et les applications qui s'y exécutent. Ils contiennent des informations qui aident à résoudre les problèmes ou à surveiller les fonctions du système. Le système de journalisation de Red Hat Enterprise Linux est basé sur le protocole intégré **syslog**. Des programmes particuliers utilisent ce système pour enregistrer des événements et les organiser dans des fichiers journaux, qui sont utiles lors de l'audit du système d'exploitation et de la résolution de divers problèmes.

9.1. SERVICES TRAITANT LES MESSAGES SYSLOG

Les deux services suivants traitent les messages **syslog**:

- Le démon **systemd-journald**
- Le service **Rsyslog**

Le démon **systemd-journald** collecte les messages provenant de diverses sources et les transmet à **Rsyslog** pour traitement ultérieur. Le démon **systemd-journald** collecte les messages provenant des sources suivantes :

- Noyau
- Premiers stades du processus de démarrage
- Sortie standard et sortie d'erreur des démons lors de leur démarrage et de leur exécution
- **Syslog**

Le service **Rsyslog** trie les messages **syslog** par type et par priorité et les écrit dans les fichiers du répertoire **/var/log**. Le répertoire **/var/log** stocke de manière persistante les messages du journal.

9.2. SOUS-RÉPERTOIRES STOCKANT LES MESSAGES SYSLOG

Les sous-répertoires suivants du répertoire **/var/log** stockent les messages **syslog**.

- **/var/log/messages** - tous les messages **syslog** à l'exception des suivants
- **/var/log/secure** - messages et erreurs liés à la sécurité et à l'authentification
- **/var/log/maillog** - messages et erreurs liés au serveur de messagerie
- **/var/log/cron** - les fichiers journaux relatifs aux tâches exécutées périodiquement
- **/var/log/boot.log** - les fichiers journaux relatifs au démarrage du système

9.3. INSPECTION DES FICHIERS JOURNAUX À L'AIDE DE LA CONSOLE WEB

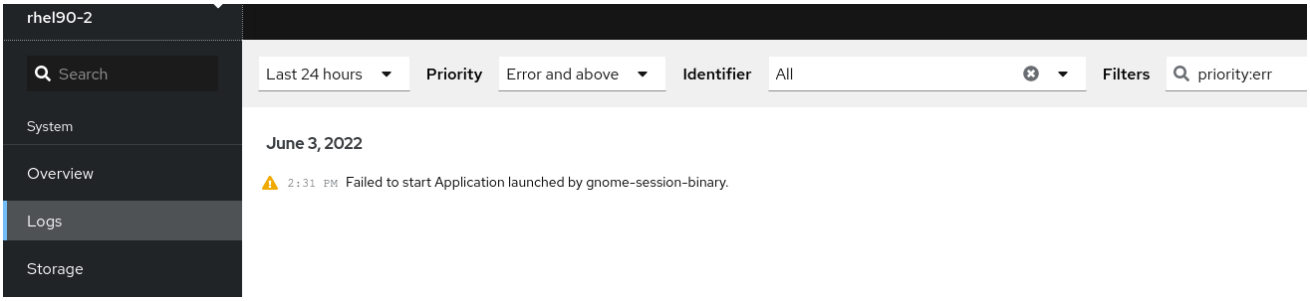
Suivez les étapes de cette procédure pour inspecter les fichiers journaux à l'aide de la console web RHEL.

Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.

2. Cliquez sur **Logs**.

Figure 9.1. Inspection des fichiers journaux dans la console web RHEL 9



9.4. CONSULTATION DES JOURNAUX À L'AIDE DE LA LIGNE DE COMMANDE

Le Journal est un composant de systemd qui permet de visualiser et de gérer les fichiers journaux. Il résout les problèmes liés à la journalisation traditionnelle, est étroitement intégré au reste du système et prend en charge diverses technologies de journalisation ainsi que la gestion de l'accès aux fichiers de journalisation.

Vous pouvez utiliser la commande **journalctl** pour consulter les messages du journal du système à l'aide de la ligne de commande, par exemple :

```
$ journalctl -b | grep kvm
May 15 11:31:41 localhost.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
May 15 11:31:41 localhost.localdomain kernel: kvm-clock: cpu 0, msr 76401001, primary cpu clock
...
```

Tableau 9.1. Visualisation des informations sur le système

Commandement	Description
journalctl	Affiche toutes les entrées de journal collectées.
journalctl FILEPATH	Affiche les journaux relatifs à un fichier spécifique. Par exemple, la commande **journalctl /dev/sda** affiche les journaux relatifs au système de fichiers **/dev/sda**.
journalctl -b	Affiche les journaux pour le démarrage en cours.
journalctl -k -b -1	Affiche les journaux du noyau pour le démarrage en cours.

Tableau 9.2. Consultation d'informations sur des services spécifiques

Commandement	Description
journalctl -b _SYSTEMD_UNIT=foo	Filtrer le journal pour voir ceux qui correspondent au service \N "foo" **systemd**.
journalctl -b _SYSTEMD_UNIT=foo _PID=number	Combine les correspondances. Par exemple, cette commande affiche les journaux de **systemd-units** qui correspondent à **foo** et au PID**number**.
journalctl -b _SYSTEMD_UNIT=foo _PID=number _SYSTEMD_UNIT=foo1	Le séparateur " " combine deux expressions dans un OU logique. Par exemple, cette commande affiche tous les messages du processus de service **foo** avec le processus **PID** plus tous les messages du service **foo1** (à partir de n'importe lequel de ses processus).
journalctl -b _SYSTEMD_UNIT=foo _SYSTEMD_UNIT=foo1	Cette commande affiche toutes les entrées correspondant à l'une ou l'autre expression, se référant au même champ. Ici, cette commande affiche les journaux correspondant à l'unité système **foo** ou à l'unité système**foo1**.

Tableau 9.3. Visualisation des journaux relatifs à des bottes spécifiques

Commandement	Description
journalctl --list-boots	Affiche une liste tabulaire des numéros d'amorçage, de leurs identifiants et des horodatages du premier et du dernier message relatifs à l'amorçage. Vous pouvez utiliser l'ID dans la commande suivante pour obtenir des informations détaillées.
journalctl --boot=ID _SYSTEMD_UNIT=foo	Affiche des informations sur l'ID de démarrage spécifié.

9.5. RESSOURCES SUPPLÉMENTAIRES

- **man journalctl(1)**
- Configuration d'une solution de journalisation à distance

CHAPITRE 10. ACCÉDER À L'ASSISTANCE DE RED HAT

Cette section décrit comment résoudre efficacement vos problèmes à l'aide de l'assistance de Red Hat et de **sosreport**.

Pour obtenir une assistance de Red Hat, utilisez le portail client de Red Hat , qui donne accès à tout ce qui est disponible avec votre abonnement.

10.1. OBTENIR L'ASSISTANCE DE RED HAT VIA LE PORTAIL CLIENT DE RED HAT

La section suivante décrit comment utiliser le portail client de Red Hat pour obtenir de l'aide.

Conditions préalables

- Un compte utilisateur valide sur le portail client Red Hat. Voir Créer un login Red Hat .
- Un abonnement actif pour le système RHEL.

Procédure

1. Accéder à l'assistance de Red Hat :
   a. Ouvrir un nouveau dossier d'assistance.
   b. Lancez un chat en direct avec un expert Red Hat.
   c. Contactez un expert Red Hat en l'appelant ou en lui envoyant un e-mail.

10.2. RÉSOLUTION DES PROBLÈMES LIÉS À L'UTILISATION DE SOSREPORT

La commande **sosreport** collecte des détails de configuration, des informations sur le système et des informations de diagnostic à partir d'un système Red Hat Enterprise Linux.

La section suivante décrit comment utiliser la commande **sosreport** pour produire des rapports pour vos cas d'assistance.

Conditions préalables

- Un compte utilisateur valide sur le portail client Red Hat. Voir Créer un login Red Hat .
- Un abonnement actif pour le système RHEL.
- Un numéro de dossier d'assistance.

Procédure

1. Installez le paquetage **sos**:

```
# dnf install sos
```

NOTE

L'installation minimale par défaut de Red Hat Enterprise Linux n'inclut pas le paquetage **sos**, qui fournit la commande **sosreport**.

2. Générer un rapport :

```
# sosreport
```

3. Joignez le rapport à votre dossier d'appui.
   Consultez l'article Comment puis-je joindre un fichier à un dossier d'assistance de Red Hat ? De la base de connaissances de Red Hat pour plus d'informations.

   Notez que lorsque vous joignez le rapport, vous êtes invité à saisir le numéro du cas d'assistance concerné.

Ressources supplémentaires

- Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

CHAPITRE 11. INTRODUCTION À SYSTEMD

En tant qu'administrateur système, vous pouvez gérer les aspects critiques de votre système avec **systemd**. Servant de gestionnaire de système et de service pour les systèmes d'exploitation Linux, la suite logicielle **systemd** fournit des outils et des services pour le contrôle, la création de rapports et l'initialisation du système. Les principales caractéristiques de **systemd** sont les suivantes

- Démarrage parallèle des services du système pendant le démarrage
- Activation à la demande des démons
- Logique de contrôle des services basée sur la dépendance

L'objet de base que **systemd** gère est une unité *systemd unit*, une représentation des ressources et des services du système. Une unité **systemd** se compose d'un nom, d'un type et d'un fichier de configuration qui définit et gère une tâche particulière. Vous pouvez utiliser les fichiers d'unité pour configurer le comportement du système. Voir les exemples suivants de différents types d'unités systemd :

Service
: Contrôle et gère les différents services du système.

Cible
: Représente un groupe d'unités qui définissent les états du système.

Dispositif
: Gérer les dispositifs matériels et leur disponibilité.

Montage
: Gère le montage du système de fichiers.

Minuterie
: Planifie l'exécution de tâches à des intervalles spécifiques.

NOTE

Pour afficher tous les types d'unités disponibles :

```
# systemctl -t help
```

11.1. EMPLACEMENT DES FICHIERS DE L'UNITÉ SYSTEMD

Les fichiers de configuration de l'unité se trouvent dans l'un des répertoires suivants :

Tableau 11.1. emplacement des fichiers de l'unité systemd

Annuaire	Description
/usr/lib/systemd/system/	**systemd** distribués avec les paquets RPM installés.
/run/systemd/system/	**systemd** créés au moment de l'exécution. Ce répertoire est prioritaire sur le répertoire contenant les fichiers d'unités de service installés.

Annuaire	Description
/etc/systemd/system/	**systemd** les fichiers d'unités créés à l'aide de la commande **systemctl enable** ainsi que les fichiers d'unités ajoutés lors de l'extension d'un service. Ce répertoire est prioritaire sur le répertoire contenant les fichiers unitaires d'exécution.

La configuration par défaut de **systemd** est définie lors de la compilation et se trouve dans le fichier **/etc/systemd/system.conf**. En éditant ce fichier, vous pouvez modifier la configuration par défaut en remplaçant globalement les valeurs des unités **systemd**.

Par exemple, pour remplacer la valeur par défaut du délai d'attente, qui est fixé à 90 secondes, utilisez le paramètre **DefaultTimeoutStartSec** pour saisir la valeur requise en secondes.

```
DefaultTimeoutStartSec= (délai de démarrage par défaut)required value
```

CHAPITRE 12. GÉRER LES SERVICES SYSTÈME AVEC SYSTEMCTL

En tant qu'administrateur système, vous pouvez gérer les services système à l'aide de l'utilitaire **systemctl**. Vous pouvez effectuer diverses tâches, telles que le démarrage, l'arrêt et le redémarrage des services en cours d'exécution, l'activation et la désactivation des services à démarrer au démarrage, l'établissement d'une liste des services disponibles et l'affichage de l'état des services du système.

12.1. SERVICES DU SYSTÈME D'INSCRIPTION

Vous pouvez dresser la liste de toutes les unités de service actuellement chargées et afficher l'état de toutes les unités de service disponibles.

Procédure

Utilisez la commande **systemctl** pour effectuer l'une des tâches suivantes :

- Liste de toutes les unités de service actuellement chargées :

```
$ systemctl list-units --type service
UNIT                    LOAD   ACTIVE SUB     DESCRIPTION
abrt-ccpp.service       loaded active exited  Install ABRT coredump hook
abrt-oops.service       loaded active running ABRT kernel log watcher
abrtd.service           loaded active running ABRT Automated Bug Reporting Tool
...
systemd-vconsole-setup.service loaded active exited  Setup Virtual Console
tog-pegasus.service           loaded active running OpenPegasus CIM Server

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

46 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'
```

  Par défaut, la commande **systemctl list-units** n'affiche que les unités actives. Pour chaque fichier d'unité de service, la commande fournit un aperçu des paramètres suivants :

  UNIT

  Le nom complet de l'unité de service

  LOAD

  L'état de chargement du fichier de configuration

  ACTIVE ou SUB

  L'état actuel d'activation des fichiers d'unité de haut niveau et de bas niveau

  DESCRIPTION

  Une brève description de l'objectif et de la fonctionnalité de l'unité

- Lister **all loaded units regardless of their state** en utilisant la commande suivante avec l'option de ligne de commande **--all** ou **-a**:

```
$ systemctl list-units --type service --all
```

- Liste l'état (**enabled** ou **disabled**) de toutes les unités de service disponibles :

```
$ systemctl list-unit-files --type service
UNIT FILE                              STATE
abrt-ccpp.service                      enabled
abrt-oops.service                      enabled
abrtd.service                          enabled
...
wpa_supplicant.service                 disabled
ypbind.service                         disabled

208 unit files listed.
```

Pour chaque unité de service, cette commande affiche :

UNIT FILE

Le nom complet de l'unité de service

STATE

L'information indiquant si l'unité de service est activée ou désactivée pour démarrer automatiquement pendant le démarrage

Ressources supplémentaires

- Affichage de l'état des services du système

12.2. AFFICHAGE DE L'ÉTAT DES SERVICES DU SYSTÈME

Vous pouvez inspecter n'importe quelle unité de service pour obtenir des informations détaillées et vérifier l'état du service, qu'il soit activé pour démarrer au démarrage ou en cours d'exécution. Vous pouvez également visualiser les services dont le démarrage est ordonné après ou avant une unité de service particulière.

Procédure

Utilisez la commande **systemctl** pour effectuer l'une des tâches suivantes :

- Affiche des informations détaillées sur une unité de service correspondant à un service système :

```
$ systemctl status <name>.service
```

Remplacez ***<name>*** par le nom de l'unité de service que vous souhaitez inspecter (par exemple, **gdm**).

Cette commande permet d'afficher les informations suivantes :

  - Le nom de l'unité de service sélectionnée suivi d'une brève description
  - Un ou plusieurs champs décrits dans Informations sur l'unité de service disponible
  - L'exécution de l'unité de service : si l'unité est exécutée par l'utilisateur **root**
  - Les entrées de journal les plus récentes

Tableau 12.1. Informations sur les unités de service disponibles

Field	Description
Loaded	Informations indiquant si l'unité de service a été chargée, le chemin d'accès absolu au fichier de l'unité et une note indiquant si l'unité est autorisée à démarrer pendant l'amorçage.
Active	Information indiquant si l'unité de service est en cours d'exécution, suivie d'un horodatage.
Main PID	L'ID du processus et le nom du service système correspondant.
Status	Informations supplémentaires sur le service système correspondant.
Process	Informations supplémentaires sur les processus connexes.
CGroup	Informations supplémentaires sur les groupes de contrôle apparentés (**cgroups**).

Exemple 12.1. Affichage de l'état des services

L'unité de service pour le gestionnaire d'affichage GNOME est nommée **gdm.service**. Pour déterminer l'état actuel de cette unité de service, tapez ce qui suit à l'invite de l'interpréteur de commandes :

```
# systemctl status gdm.service
gdm.service - GNOME Display Manager
   Loaded: loaded (/usr/lib/systemd/system/gdm.service; enabled)
   Active: active (running) since Thu 2013-10-17 17:31:23 CEST; 5min ago
 Main PID: 1029 (gdm)
   CGroup: /system.slice/gdm.service
           ├─1029 /usr/sbin/gdm
           └─1047 /usr/bin/Xorg :0 -background none -verbose -auth /r...

Oct 17 17:31:23 localhost systemd[1]: Started GNOME Display Manager.
```

- Vérifier qu'une unité de service particulière fonctionne :

```
$ systemctl is-active <name>.service
```

- Déterminez si une unité de service particulière est autorisée à démarrer pendant l'amorçage :

```
$ systemctl is-enabled <name>.service
```

NOTE

Les commandes **systemctl is-active** et **systemctl is-enabled** renvoient un état de sortie de **0** si l'unité de service spécifiée est en cours d'exécution ou activée.

- Vérifier quels sont les services que **systemd** ordonne de démarrer avant l'unité de service spécifiée

```
# systemctl list-dependencies --after <name>.service
```

Par exemple, pour afficher la liste des services dont le démarrage a été ordonné avant **gdm**, entrez :

```
# systemctl list-dependencies --after gdm.service
gdm.service
├─dbus.socket
├─getty@tty1.service
├─livesys.service
├─plymouth-quit.service
├─system.slice
├─systemd-journald.socket
├─systemd-user-sessions.service
└─basic.target
[output truncated]
```

- Vérifiez quels services **systemd** ordonne de démarrer après l'unité de service spécifiée :

```
# systemctl list-dependencies --before <name>.service
```

Par exemple, pour afficher la liste des services que **systemd** ordonne de lancer après **gdm**, entrez :

```
# systemctl list-dependencies --before gdm.service
gdm.service
├─dracut-shutdown.service
├─graphical.target
│ ├─systemd-readahead-done.service
│ ├─systemd-readahead-done.timer
│ └─systemd-update-utmp-runlevel.service
└─shutdown.target
  ├─systemd-reboot.service
  └─final.target
    └─systemd-reboot.service
```

Ressources supplémentaires

- Services du système d'inscription

12.3. DÉMARRAGE D'UN SERVICE SYSTÈME

Vous pouvez démarrer le service système dans la session en cours à l'aide de la commande **start**.

Conditions préalables

- Accès à la racine

Procédure

- Démarrer un service système dans la session en cours :

```
# systemctl start <name>.service
```

Remplacez ***<name>*** par le nom de l'unité de service que vous souhaitez démarrer (par exemple, **httpd.service**).

NOTE

Sur **systemd**, il existe des dépendances positives et négatives entre les services. Le démarrage d'un service particulier peut nécessiter le démarrage d'un ou de plusieurs autres services (**positive dependency**) ou l'arrêt d'un ou de plusieurs services (**negative dependency**).

Lorsque vous tentez de démarrer un nouveau service, **systemd** résout toutes les dépendances automatiquement, sans notification explicite à l'utilisateur. Cela signifie que si vous exécutez déjà un service et que vous tentez de démarrer un autre service avec une dépendance négative, le premier service est automatiquement arrêté.

Par exemple, si vous exécutez le service **postfix** et que vous tentez de démarrer le service **sendmail**, **systemd** arrête d'abord automatiquement **postfix**, car ces deux services sont en conflit et ne peuvent pas s'exécuter sur le même port.

Ressources supplémentaires

- **systemctl(1)** page de manuel
- Activation d'un service système
- Affichage de l'état des services du système

12.4. ARRÊT D'UN SERVICE SYSTÈME

Si vous souhaitez arrêter un service système dans la session en cours, utilisez la commande **stop**.

Conditions préalables

- Accès à la racine

Procédure

- Arrêter un service système :

```
# systemctl stop <name>.service
```

Remplacez ***<name>*** par le nom de l'unité de service que vous souhaitez arrêter (par exemple, **bluetooth**).

Ressources supplémentaires

- **systemctl(1)** page de manuel
- Désactivation d'un service système
- Affichage de l'état des services du système

12.5. REDÉMARRAGE D'UN SERVICE SYSTÈME

Vous pouvez redémarrer le service système dans la session en cours à l'aide de la commande **restart** pour effectuer les actions suivantes :

- Arrêter l'unité de service sélectionnée dans la session en cours et la redémarrer immédiatement.
- Redémarrer une unité de service uniquement si le service correspondant est déjà en cours d'exécution.
- Recharger la configuration d'un service système sans en interrompre l'exécution.

Conditions préalables

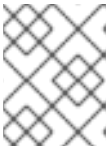
- Accès à la racine

Procédure

- Redémarrer un service système :

```
# systemctl restart <name>.service
```

Remplacez ***<name>*** par le nom de l'unité de service que vous souhaitez redémarrer (par exemple, **httpd**).



NOTE

Si l'unité de service sélectionnée n'est pas en cours d'exécution, cette commande la démarre également.

- Facultatif : Redémarrer une unité de service uniquement si le service correspondant est déjà en cours d'exécution :

```
# systemctl try-restart <name>.service
```

- Facultatif : Recharger la configuration sans interrompre l'exécution du service :

```
# systemctl reload <name>.service
```

NOTE

Les services système qui ne prennent pas en charge cette fonctionnalité ignorent cette commande. Pour redémarrer ces services, utilisez plutôt les commandes **reload-or-restart** et **reload-or-try-restart**.

Ressources supplémentaires

- **systemctl** page de manuel
- Affichage de l'état des services du système

12.6. ACTIVATION DU DÉMARRAGE D'UN SERVICE SYSTÈME AU DÉMARRAGE

Vous pouvez activer un service pour qu'il démarre automatiquement au démarrage, ces changements s'appliquant au prochain redémarrage.

Conditions préalables

- Accès à la racine
- Le service que vous voulez activer ne doit pas être masqué. Si vous avez un service masqué, démasquez-le d'abord :

```
# systemctl unmask <name>.service
```

Procédure

- Activer un service pour qu'il démarre au démarrage :

```
# systemctl enable <name>.service
```

  Remplacez ***<name>*** par le nom de l'unité de service que vous souhaitez activer (par exemple, **httpd**).

- Facultatif : vous pouvez également activer et démarrer un service à l'aide d'une seule commande :

```
# systemctl enable --now <name>.service
```

Ressources supplémentaires

- **systemctl (1)** page de manuel
- Affichage de l'état des services du système
- Démarrage d'un service système

12.7. DÉSACTIVATION DU DÉMARRAGE D'UN SERVICE SYSTÈME AU DÉMARRAGE

Vous pouvez empêcher une unité de service de démarrer automatiquement au moment du démarrage. Si vous désactivez un service, il ne démarrera pas au démarrage, mais vous pouvez le démarrer manuellement. Vous pouvez également masquer un service afin qu'il ne puisse pas être démarré manuellement. Le masquage est une façon de désactiver un service qui le rend définitivement inutilisable jusqu'à ce qu'il soit à nouveau démasqué.

Conditions préalables

- Accès à la racine

Procédure

- Désactiver un service pour qu'il démarre au démarrage :

```
# systemctl disable <name>.service
```

Remplacez ***<name>*** par le nom de l'unité de service que vous souhaitez désactiver (par exemple, **bluetooth**).

- Facultatif : si vous souhaitez rendre un service définitivement inutilisable, masquez-le :

```
# systemctl mask <name>.service
```

Cette commande remplace le fichier **/etc/systemd/system/*name*.service** par un lien symbolique vers **/dev/null**, rendant le fichier d'unité actuel inaccessible à **systemd**.

Ressources supplémentaires

- **systemctl (1)** page de manuel
- Affichage de l'état des services du système
- Arrêt d'un service système

CHAPITRE 13. DÉMARRAGE DANS UN ÉTAT DU SYSTÈME CIBLE

En tant qu'administrateur système, vous pouvez contrôler le processus de démarrage de votre système et définir l'état dans lequel vous souhaitez qu'il démarre. C'est ce qu'on appelle une cible **systemd**, et c'est un ensemble d'unités **systemd** que votre système démarre pour atteindre un certain niveau de fonctionnalité. Lorsque vous travaillez avec les cibles systemd, vous pouvez afficher la cible par défaut, sélectionner une cible au moment de l'exécution, modifier la cible de démarrage par défaut, démarrer dans une cible d'urgence ou de secours.

13.1. FICHIERS DE L'UNITÉ CIBLE

Les cibles dans **systemd** sont des groupes d'unités liées qui agissent comme des points de synchronisation pendant le démarrage de votre système. Les fichiers d'unités cibles, qui se terminent par l'extension **.target**, représentent les cibles **systemd**. L'objectif des unités cibles est de regrouper diverses unités **systemd** par le biais d'une chaîne de dépendances.

Prenons les exemples suivants :

- Le site **graphical.target unit** permet de démarrer une session graphique, de lancer des services système tels que le gestionnaire d'affichage GNOME (**gdm.service**) ou le service des comptes (**accounts-daemon.service**), et d'activer le site **multi-user.target unit**.
- De même, l'unité **multi-user.target** démarre d'autres services essentiels du système tels que NetworkManager (**NetworkManager.service**) ou D-Bus (**dbus.service**) et active une autre unité cible nommée **basic.target**.

Vous pouvez définir les cibles **systemd** suivantes comme cibles par défaut ou cibles actuelles :

Tableau 13.1. Cibles communes systemd

sauvetage	cible d'unité qui tire le système de base et génère une coquille de sauvetage
multi-utilisateurs	objectif de l'unité pour la mise en place d'un système multi-utilisateurs
graphique	cible unitaire pour la mise en place d'un écran de connexion graphique
d'urgence	cible unitaire qui lance un shell d'urgence sur la console principale

Ressources supplémentaires

- **systemd.special(7)** page de manuel
- **systemd.target(5)** page de manuel

13.2. MODIFIER LA CIBLE PAR DÉFAUT POUR DÉMARRER

Au démarrage du système, **systemd** active le lien symbolique **default.target**, qui pointe vers la véritable unité cible. Vous trouverez l'unité cible par défaut actuellement sélectionnée dans le fichier **/etc/systemd/system/default.target**. Chaque unité cible représente un certain niveau de fonctionnalité et est utilisée pour regrouper d'autres unités. En outre, les unités cibles servent de points de

synchronisation pendant le démarrage. Vous pouvez modifier la cible par défaut dans laquelle votre système démarre. Lorsque vous définissez une unité cible par défaut, la cible actuelle reste inchangée jusqu'au prochain redémarrage.

Conditions préalables

- Accès à la racine

Procédure

1. Déterminez l'unité cible par défaut que **systemd** utilise pour démarrer le système :

```
# systemctl get-default
graphical.target
```

2. Liste des cibles actuellement chargées :

```
# systemctl list-units --type target
```

3. Configurer le système pour qu'il utilise une autre unité cible par défaut :

```
# systemctl set-default <name>.target
```

Remplacer ***<name>*** par le nom de l'unité cible que vous souhaitez utiliser par défaut.

```
Example:
# systemctl set-default multi-user.target
Removed /etc/systemd/system/default.target
Created symlink /etc/systemd/system/default.target -> /usr/lib/systemd/system/multi-user.target
```

4. Vérifiez l'unité cible par défaut :

```
# systemctl get-default
multi-user.target
```

5. Appliquez les modifications en redémarrant :

```
# reboot
```

Ressources supplémentaires

- **systemctl(1)** page de manuel
- **systemd.special(7)** page de manuel
- **bootup(7)** page de manuel

13.3. MODIFIER LA CIBLE ACTUELLE

Sur un système en cours d'exécution, vous pouvez changer d'unité cible dans le démarrage en cours sans redémarrer. Si vous passez à une autre cible, **systemd** démarre tous les services et leurs

dépendances dont cette cible a besoin, et arrête tous les services que la nouvelle cible n'active pas. L'isolation d'une cible différente n'affecte que le démarrage en cours.

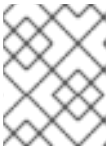
Procédure

1. Facultatif : Déterminer la cible actuelle :

```
# systemctl get-default
graphical.target
```

2. Facultatif : Affiche la liste des cibles que vous pouvez sélectionner :

```
# systemctl list-units --type target
```



NOTE

Vous ne pouvez isoler que les cibles pour lesquelles l'option **AllowIsolate=yes** a été définie dans les fichiers d'unité.

3. Passer à une autre unité cible dans le démarrage en cours :

```
# systemctl isolate <name>.target
```

Remplacez *<name>* par le nom de l'unité cible que vous souhaitez utiliser dans le démarrage en cours.

```
Example:
# systemctl isolate multi-user.target
```

Cette commande démarre l'unité cible nommée **multi-user** et toutes les unités dépendantes, et arrête immédiatement toutes les autres unités.

Ressources supplémentaires

- **systemctl(1)** page de manuel

13.4. DÉMARRAGE EN MODE DE SECOURS

Vous pouvez démarrer sur le site *rescue mode* qui fournit un environnement mono-utilisateur pour le dépannage ou la réparation si le système ne peut pas atteindre une cible ultérieure et que le processus de démarrage normal échoue. En mode de secours, le système tente de monter tous les systèmes de fichiers locaux et de démarrer certains services système importants, mais il n'active pas les interfaces réseau.

Conditions préalables

- Accès à la racine

Procédure

- Pour entrer dans le mode sauvetage, changez la cible actuelle dans la session en cours :

```
# systemctl rescue

Broadcast message from root@localhost on pts/0 (Fri 2023-03-24 18:23:15 CEST):

The system is going down to rescue mode NOW!
```

NOTE

Cette commande est similaire à **systemctl isolate rescue.target**, mais elle envoie également un message d'information à tous les utilisateurs actuellement connectés au système.

Pour empêcher **systemd** d'envoyer un message, entrez la commande suivante avec l'option de ligne de commande **--no-wall**:

```
# systemctl --no-wall rescue
```

Étapes de dépannage

Si votre système n'est pas en mesure d'entrer dans le mode de secours, vous pouvez démarrer sur *emergency mode*, qui fournit l'environnement le plus minimal possible. En mode d'urgence, le système monte le système de fichiers racine uniquement pour la lecture, n'essaie pas de monter d'autres systèmes de fichiers locaux, n'active pas les interfaces réseau et ne démarre que quelques services essentiels.

13.5. DÉPANNAGE DU PROCESSUS DE DÉMARRAGE

En tant qu'administrateur système, vous pouvez sélectionner une cible autre que la cible par défaut au moment du démarrage afin de résoudre les problèmes liés au processus de démarrage. La modification de la cible au moment du démarrage n'affecte qu'un seul démarrage. Vous pouvez démarrer sur *emergency mode*, qui offre l'environnement le plus minimal possible.

Procédure

1. Redémarrez le système et interrompez le compte à rebours du menu du chargeur de démarrage en appuyant sur n'importe quelle touche, à l'exception de la touche Entrée, qui lancerait un démarrage normal.

2. Déplacez le curseur sur l'entrée du noyau que vous souhaitez lancer.

3. Appuyez sur la touche E pour modifier l'entrée actuelle.

4. Déplacez-vous à la fin de la ligne qui commence par **linux** et appuyez sur Ctrl E pour sauter à la fin de la ligne :

```
linux ($root)/vmlinuz-5.14.0-70.22.1.e19_0.x86_64 root=/dev/mapper/rhel-root ro crash\
kernel=auto resume=/dev/mapper/rhel-swap rd.lvm.lv/swap rhgb quiet
```

5. Pour choisir une autre cible de démarrage, ajoutez le paramètre **systemd.unit=** à la fin de la ligne commençant par **linux**:

```
linux ($root)/vmlinuz-5.14.0-70.22.1.e19_0.x86_64 root=/dev/mapper/rhel-root ro crash\
kernel=auto resume=/dev/mapper/rhel-swap rd.lvm.lv/swap rhgb quiet
systemd.unit=<name>.target
```

Remplacer ***<name>*** par le nom de l'unité cible que vous souhaitez utiliser. Par exemple, **systemd.unit=emergency.target**

6. Appuyez sur Ctrl X pour démarrer avec ces paramètres.

CHAPITRE 14. ARRÊT, SUSPENSION ET MISE EN VEILLE PROLONGÉE DU SYSTÈME

En tant qu'administrateur système, vous pouvez utiliser différentes options de gestion de l'alimentation pour gérer la consommation d'énergie, effectuer un arrêt correct pour garantir que toutes les données sont sauvegardées, ou redémarrer le système pour appliquer les changements et les mises à jour.

14.1. ARRÊT DU SYSTÈME

Pour arrêter le système, vous pouvez soit utiliser directement l'utilitaire **systemctl**, soit appeler cet utilitaire par le biais de la commande **shutdown**.

L'utilisation du site **shutdown** présente les avantages suivants :

- Vous pouvez planifier un arrêt en utilisant l'argument **time**. Cela permet également d'avertir les utilisateurs qu'un arrêt du système a été programmé.
- Vous pouvez annuler l'arrêt.

Ressources supplémentaires

- Vue d'ensemble des commandes de gestion de l'énergie avec systemctl

14.2. PROGRAMMATION DE L'ARRÊT DU SYSTÈME

En tant qu'administrateur système, vous pouvez programmer un arrêt différé pour donner aux utilisateurs le temps de sauvegarder leur travail et de se déconnecter du système. Utilisez la commande **shutdown** pour effectuer les opérations suivantes :

- Arrêter le système et mettre la machine hors tension à une certaine heure
- Arrêter le système sans mettre la machine hors tension
- Annuler un arrêt en cours

Conditions préalables

- Accès à la racine

Procédure

Utilisez la commande **shutdown** pour effectuer l'une des tâches suivantes :

- Indiquez l'heure à laquelle vous souhaitez arrêter le système et mettre la machine hors tension :

```
# shutdown --poweroff hh:mm
```

Où ***hh:mm*** est l'heure en notation de 24 heures. Pour empêcher toute nouvelle connexion, le fichier **/run/nologin** est créé 5 minutes avant l'arrêt du système.

Lorsque vous utilisez l'argument time, vous pouvez avertir les utilisateurs connectés au système de l'arrêt planifié en spécifiant une option *wall message*, par exemple **shutdown --poweroff 13:59 "Attention. The system will shut down at 13:59"**.

- Arrêter et stopper le système après un délai, sans mettre la machine hors tension :

```
# shutdown --halt m
```

  Où ***m*** est le délai en minutes. Vous pouvez utiliser le mot-clé **now** comme alias de **0**.

- Annuler un arrêt en cours :

```
# shutdown -c
```

Ressources supplémentaires

- **shutdown(8)** page du manuel
- Arrêter le système à l'aide de la commande systemctl

14.3. ARRÊTER LE SYSTÈME À L'AIDE DE LA COMMANDE SYSTEMCTL

En tant qu'administrateur système, vous pouvez arrêter le système et mettre la machine hors tension ou arrêter le système sans mettre la machine hors tension à l'aide de la commande **systemctl**.

Conditions préalables

- Accès à la racine

Procédure

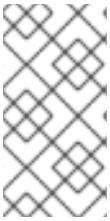
Utilisez la commande **systemctl** pour effectuer l'une des tâches suivantes :

- Arrêtez le système et mettez la machine hors tension :

```
# systemctl poweroff
```

- Arrêter le système sans mettre la machine hors tension :

```
# systemctl halt
```



NOTE

Par défaut, l'exécution de l'une ou l'autre de ces commandes entraîne l'envoi par **systemd** d'un message d'information à tous les utilisateurs actuellement connectés au système. Pour empêcher **systemd** d'envoyer ce message, exécutez la commande sélectionnée avec l'option de ligne de commande **--no-wall**.

14.4. REDÉMARRAGE DU SYSTÈME

Lorsque vous redémarrez le système, **systemd** arrête tous les programmes et services en cours, le système s'éteint, puis redémarre immédiatement. Le redémarrage du système peut être utile dans les situations suivantes :

- Après l'installation d'un nouveau logiciel ou d'une mise à jour
- Après avoir modifié les paramètres du système

- Lors de la résolution des problèmes liés au système

Conditions préalables

- Accès à la racine

Procédure

- Redémarrer le système :

```
# systemctl reboot
```

NOTE

Par défaut, lorsque vous utilisez cette commande, **systemd** envoie un message d'information à tous les utilisateurs actuellement connectés au système. Pour empêcher **systemd** d'envoyer ce message, exécutez cette commande avec l'option **--no-wall**.

14.5. OPTIMISER LA CONSOMMATION D'ÉNERGIE EN SUSPENDANT ET EN METTANT EN VEILLEUSE LE SYSTÈME

En tant qu'administrateur système, vous pouvez gérer la consommation d'énergie, économiser de l'énergie sur vos systèmes et préserver l'état actuel de votre système. Pour ce faire, appliquez l'un des modes suivants :

Suspendre

La suspension sauvegarde l'état du système dans la RAM et, à l'exception du module RAM, met hors tension la plupart des périphériques de la machine. Lorsque vous rallumez la machine, le système restaure son état à partir de la RAM sans avoir à redémarrer. Comme l'état du système est sauvegardé dans la RAM et non sur le disque dur, la restauration du système à partir du mode suspension est nettement plus rapide qu'à partir de l'hibernation. Cependant, l'état du système suspendu est également vulnérable aux coupures de courant.

Hibernation

L'hibernation permet de sauvegarder l'état du système sur le disque dur et de mettre l'ordinateur hors tension. Lorsque vous rallumez la machine, le système restaure son état à partir des données sauvegardées sans avoir à redémarrer. Comme l'état du système est sauvegardé sur le disque dur et non dans la mémoire vive, la machine n'a pas besoin de maintenir l'alimentation électrique du module RAM. Toutefois, la restauration du système à partir de l'hibernation est nettement plus lente que la restauration à partir du mode suspension.

Sommeil hybride

Il combine des éléments de l'hibernation et de la suspension. Le système enregistre d'abord l'état actuel sur le disque dur, puis entre dans un état de faible consommation similaire à la mise en veille, ce qui permet au système de se remettre en marche plus rapidement. L'avantage de la veille hybride est que si le système perd de l'énergie pendant la veille, il peut toujours récupérer l'état précédent à partir de l'image sauvegardée sur le disque dur, comme dans le cas de l'hibernation.

Suspendre, puis hiberner

Ce mode suspend d'abord le système, ce qui a pour effet de sauvegarder l'état actuel du système dans la mémoire vive et de placer le système dans un mode de faible consommation d'énergie. Le système entre en hibernation s'il reste suspendu pendant une période spécifique que vous pouvez définir dans le paramètre **HibernateDelaySec**. L'hibernation enregistre l'état du système sur le

disque dur et éteint complètement le système. Le mode "suspension puis hibernation" présente l'avantage d'économiser l'énergie de la batterie tout en permettant de reprendre rapidement le travail. En outre, ce mode garantit que vos données sont sauvegardées en cas de panne de courant.

Conditions préalables

- Accès à la racine

Procédure

Choisissez la méthode appropriée pour l'économie d'énergie :

- Suspendre le système :

```
# systemctl suspend
```

- Mettre le système en hibernation :

```
# systemctl hibernate
```

- Mettre le système en veille prolongée et le suspendre :

```
# systemctl hybrid-sleep
```

- Suspendre le système, puis le mettre en veille prolongée :

```
# systemctl suspend-then-hibernate
```

14.6. VUE D'ENSEMBLE DES COMMANDES DE GESTION DE L'ÉNERGIE AVEC SYSTEMCTL

Vous pouvez utiliser la liste suivante de commandes **systemctl** pour contrôler la gestion de l'alimentation de votre système.

Tableau 14.1. Vue d'ensemble des commandes de gestion de l'énergie systemctl

systemctl commande	Description
systemctl halt	Arrête le système.
systemctl poweroff	Met le système hors tension.
systemctl reboot	Redémarre le système.
systemctl suspend	Suspend le système.
systemctl hibernate	Met le système en hibernation.
systemctl hybrid-sleep	Hibernation et suspension du système.

CHAPITRE 15. INTRODUCTION À LA GESTION DES COMPTES D'UTILISATEURS ET DE GROUPES

Le contrôle des utilisateurs et des groupes est un élément essentiel de l'administration du système Red Hat Enterprise Linux (RHEL). Chaque utilisateur RHEL possède des identifiants de connexion distincts et peut être assigné à différents groupes afin de personnaliser ses privilèges système.

15.1. INTRODUCTION AUX UTILISATEURS ET AUX GROUPES

Un utilisateur qui crée un fichier est le propriétaire de ce fichier *and* le groupe propriétaire de ce fichier. Le fichier se voit attribuer des autorisations de lecture, d'écriture et d'exécution distinctes pour le propriétaire, le groupe et les personnes extérieures à ce groupe. Le propriétaire du fichier ne peut être modifié que par l'utilisateur **root**. Les autorisations d'accès au fichier peuvent être modifiées à la fois par l'utilisateur **root** et par le propriétaire du fichier. Un utilisateur normal peut changer la propriété d'un fichier qu'il possède en faveur d'un groupe dont il est membre.

Chaque utilisateur est associé à un numéro d'identification numérique unique appelé *user ID* (**UID**). Chaque groupe est associé à un numéro d'identification unique appelé *group ID* (**GID**). Les utilisateurs d'un groupe ont les mêmes droits de lecture, d'écriture et d'exécution des fichiers appartenant à ce groupe.

15.2. CONFIGURATION DES ID D'UTILISATEURS ET DE GROUPES RÉSERVÉS

RHEL réserve les ID d'utilisateur et de groupe inférieurs à 1000 aux utilisateurs et groupes du système. Vous trouverez les ID d'utilisateur et de groupe réservés dans le paquetage **setup**. Pour afficher les ID d'utilisateur et de groupe réservés, utilisez :

```
cat /usr/share/doc/setup*/uidgid
```

Il est recommandé d'attribuer des identifiants aux nouveaux utilisateurs et groupes en commençant par 5000, car la plage réservée peut augmenter à l'avenir.

Pour que les ID attribués aux nouveaux utilisateurs commencent par défaut à 5000, modifiez les paramètres **UID_MIN** et **GID_MIN** dans le fichier **/etc/login.defs**.

Procédure

Pour modifier et faire en sorte que les ID attribués aux nouveaux utilisateurs commencent à 5000 par défaut :

1. Ouvrez le fichier **/etc/login.defs** dans un éditeur de votre choix.
2. Trouvez les lignes qui définissent la valeur minimale pour la sélection automatique de l'UID.

```
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  1000
```

3. Modifier la valeur de **UID_MIN** pour commencer à 5000.

```
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  5000
```

4. Trouvez les lignes qui définissent la valeur minimale pour la sélection automatique du GID.

```
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                  1000
```

5. Modifier la valeur de **GID_MIN** pour commencer à 5000.

```
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                  5000
```

Les UID et GID attribués dynamiquement aux utilisateurs réguliers commencent maintenant à 5000.

NOTE

Les UID et GID des utilisateurs et des groupes créés avant la modification des valeurs UID_MIN et GID_MIN ne changent pas.

Cela permettra au groupe du nouvel utilisateur d'avoir le même identifiant 5000 que l'UID et le GID.

AVERTISSEMENT

Ne pas augmenter les identifiants réservés par le système au-delà de 1000 en modifiant **SYS_UID_MAX** afin d'éviter tout conflit avec les systèmes qui conservent la limite de 1000.

15.3. GROUPES PRIVÉS D'UTILISATEURS

RHEL utilise la configuration système *user private group* (**UPG**), qui facilite la gestion des groupes UNIX. Un groupe privé d'utilisateurs est créé chaque fois qu'un nouvel utilisateur est ajouté au système. Le groupe privé d'utilisateurs porte le même nom que l'utilisateur pour lequel il a été créé et cet utilisateur est le seul membre du groupe privé d'utilisateurs.

Les UPG simplifient la collaboration sur un projet entre plusieurs utilisateurs. En outre, la configuration du système UPG permet de définir en toute sécurité des autorisations par défaut pour un fichier ou un répertoire nouvellement créé, car elle permet à la fois à l'utilisateur et au groupe dont il fait partie d'apporter des modifications au fichier ou au répertoire.

Une liste de tous les groupes est stockée dans le fichier de configuration **/etc/group**.

CHAPITRE 16. GESTION DES COMPTES D'UTILISATEURS DANS LA CONSOLE WEB

La console web RHEL offre une interface graphique qui vous permet d'exécuter un large éventail de tâches administratives sans accéder directement à votre terminal. Par exemple, vous pouvez ajouter, modifier ou supprimer des comptes d'utilisateurs du système.

Après avoir lu cette section, vous saurez

- D'où proviennent les comptes existants.
- Comment ajouter de nouveaux comptes.
- Comment définir l'expiration du mot de passe.
- Comment et quand mettre fin aux sessions des utilisateurs.

Conditions préalables

- Configurez la console web RHEL. Pour plus d'informations, reportez-vous à la section Prise en main de la console web RHEL.
- Connectez-vous à la console web RHEL avec un compte auquel des autorisations d'administrateur ont été attribuées. Pour plus d'informations, voir Connexion à la console web RHEL.

16.1. COMPTES D'UTILISATEURS DU SYSTÈME GÉRÉS DANS LA CONSOLE WEB

Avec les comptes d'utilisateurs affichés dans la console web RHEL, vous pouvez :

- Authentifier les utilisateurs lors de l'accès au système.
- Définir les droits d'accès au système.

La console web RHEL affiche tous les comptes d'utilisateurs situés dans le système. Par conséquent, vous pouvez voir au moins un compte d'utilisateur juste après la première connexion à la console web.

Après vous être connecté à la console web RHEL, vous pouvez effectuer les opérations suivantes :

- Créer de nouveaux comptes utilisateurs.
- Modifier leurs paramètres.
- Verrouiller les comptes.
- Mettre fin aux sessions des utilisateurs.

16.2. AJOUTER DE NOUVEAUX COMPTES À L'AIDE DE LA CONSOLE WEB

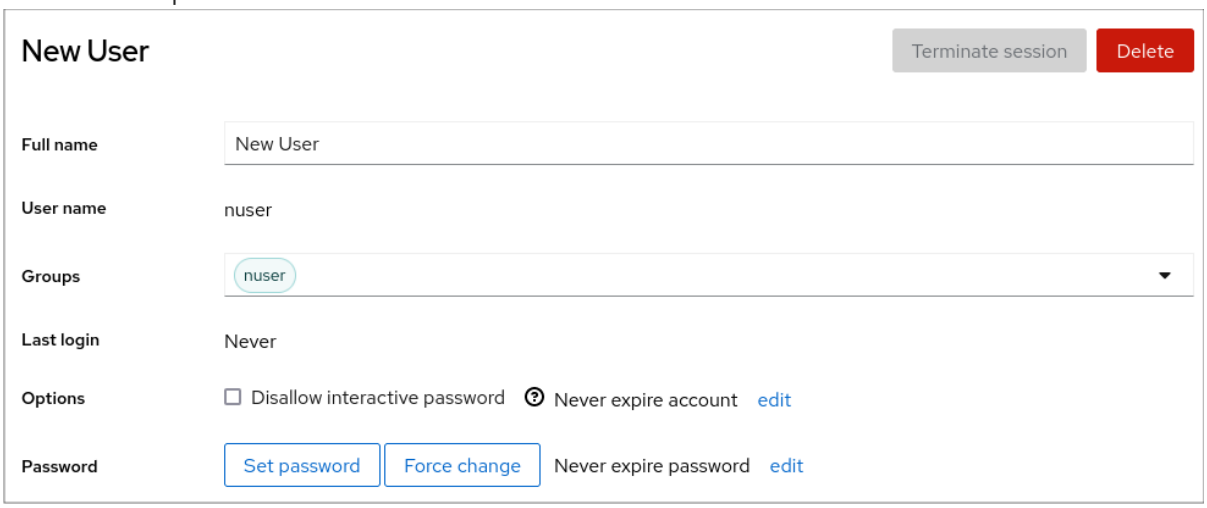
Les étapes suivantes permettent d'ajouter des comptes d'utilisateurs au système et de définir des droits d'administration pour les comptes via la console web RHEL.

Conditions préalables

- La console web RHEL doit être installée et accessible. Pour plus de détails, voir Installation de la console web.

Procédure

1. Connectez-vous à la console web RHEL.
2. Cliquez sur **Comptes**.
3. Cliquez sur **Créer un nouveau compte**.
4. Dans le champ **Full Name**, saisissez le nom complet de l'utilisateur.
   La console web RHEL suggère automatiquement un nom d'utilisateur à partir du nom complet et le remplit dans le champ **User Name**. Si vous ne souhaitez pas utiliser la convention de dénomination originale qui consiste à utiliser la première lettre du prénom et le nom de famille complet, mettez à jour la suggestion.
5. Dans les champs **Password/Confirm**, saisissez le mot de passe et retapez-le pour vérifier qu'il est correct.
   La barre de couleur située sous les champs indique le niveau de sécurité du mot de passe saisi, ce qui ne permet pas de créer un utilisateur avec un mot de passe faible.
6. Cliquez sur **Créer** pour enregistrer les paramètres et fermer la boîte de dialogue.
7. Sélectionnez le compte nouvellement créé.
8. Dans le menu déroulant **Groups**, sélectionnez les groupes que vous souhaitez ajouter au nouveau compte.



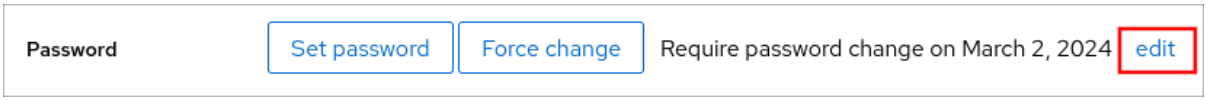
Vous pouvez maintenant voir le nouveau compte dans les paramètres de **Accounts** et vous pouvez utiliser ses informations d'identification pour vous connecter au système.

16.3. RENFORCER L'EXPIRATION DES MOTS DE PASSE DANS LA CONSOLE WEB

Par défaut, les mots de passe des comptes d'utilisateurs n'expirent jamais. Vous pouvez configurer les mots de passe du système de manière à ce qu'ils expirent après un nombre défini de jours. Lorsque le mot de passe expire, la prochaine tentative de connexion demandera un changement de mot de passe.

Procédure

1. Connectez-vous à la console web RHEL 9.
2. Cliquez sur **Comptes**.
3. Sélectionnez le compte utilisateur pour lequel vous souhaitez appliquer l'expiration du mot de passe.
4. Cliquez sur **edit** sur la ligne **Password**.



5. Dans la boîte de dialogue **Password expiration**, sélectionnez **Require password change every ... days** et entrez un nombre entier positif représentant le nombre de jours après lesquels le mot de passe expire.
6. Cliquez sur **Modifier**.
   La console web affiche immédiatement la date de la future demande de changement de mot de passe sur la ligne **Password**.

16.4. TERMINER LES SESSIONS D'UTILISATEURS DANS LA CONSOLE WEB

Un utilisateur crée des sessions utilisateur lorsqu'il se connecte au système. Mettre fin aux sessions utilisateur signifie déconnecter l'utilisateur du système. Cela peut s'avérer utile si vous devez effectuer des tâches administratives liées à des changements de configuration, par exemple des mises à niveau du système.

Dans chaque compte d'utilisateur de la console RHEL 9web, vous pouvez mettre fin à toutes les sessions du compte, à l'exception de la session de la console web que vous utilisez actuellement. Cela vous évite de perdre l'accès à votre système.

Procédure

1. Connectez-vous à la console web RHEL 9.
2. Cliquez sur **Comptes**.
3. Cliquez sur le compte utilisateur pour lequel vous souhaitez mettre fin à la session.
4. Cliquez sur **Terminer la session**.
   Si le bouton **Terminer la session** est inactif, cela signifie que l'utilisateur n'est pas connecté au système.

   La console web RHEL met fin aux sessions.

CHAPITRE 17. GESTION DES UTILISATEURS À PARTIR DE LA LIGNE DE COMMANDE

Vous pouvez gérer les utilisateurs et les groupes à l'aide de l'interface de ligne de commande (**CLI**). Cela vous permet d'ajouter, de supprimer et de modifier des utilisateurs et des groupes d'utilisateurs dans l'environnement Red Hat Enterprise Linux.

17.1. AJOUTER UN NOUVEL UTILISATEUR À PARTIR DE LA LIGNE DE COMMANDE

Cette section décrit comment utiliser l'utilitaire **useradd** pour ajouter un nouvel utilisateur.

Conditions préalables

- **Root** accès

Procédure

- Pour ajouter un nouvel utilisateur, utilisez :

```
# useradd options username
```

Remplacez *options* par les options de la ligne de commande pour la commande **useradd** et remplacez *username* par le nom de l'utilisateur.

Exemple 17.1. Ajouter un nouvel utilisateur

Pour ajouter l'utilisateur **sarah** avec l'ID d'utilisateur **5000**, utiliser :

```
# useradd -u 5000 sarah
```

Verification steps

- Pour vérifier que le nouvel utilisateur a bien été ajouté, utilisez l'utilitaire **id**.

```
# id sarah
```

La sortie revient :

```
uid=5000(sarah) gid=5000(sarah) groups=5000(sarah)
```

Ressources supplémentaires

- **useradd** page de manuel

17.2. AJOUTER UN NOUVEAU GROUPE À PARTIR DE LA LIGNE DE COMMANDE

Cette section décrit comment utiliser l'utilitaire **groupadd** pour ajouter un nouveau groupe.

Conditions préalables

- **Root** accès

Procédure

- Pour ajouter un nouveau groupe, utilisez :

```
# groupadd options group-name
```

Remplacez *options* par les options de la ligne de commande pour la commande **groupadd** et remplacez *group-name* par le nom du groupe.

Exemple 17.2. Ajouter un nouveau groupe

Pour ajouter le groupe **sysadmins** avec l'ID de groupe **5000**, utilisez :

```
# groupadd -g 5000 sysadmins
```

Verification steps

- Pour vérifier que le nouveau groupe a été ajouté, utilisez l'utilitaire **tail**.

```
# tail /etc/group
```

La sortie revient :

```
sysadmins:x:5000:
```

Ressources supplémentaires

- **groupadd** page de manuel

17.3. AJOUTER UN UTILISATEUR À UN GROUPE SUPPLÉMENTAIRE À PARTIR DE LA LIGNE DE COMMANDE

Vous pouvez ajouter un utilisateur à un groupe supplémentaire pour gérer les autorisations ou permettre l'accès à certains fichiers ou appareils.

Conditions préalables

- **root** access

Procédure

- Pour ajouter un groupe aux groupes supplémentaires de l'utilisateur, utiliser :

```
# usermod --append -G group-name username
```

Remplacez *group-name* par le nom du groupe et *username* par le nom de l'utilisateur.

Exemple 17.3. Ajouter un utilisateur à un groupe supplémentaire

Pour ajouter l'utilisateur **sysadmin** au groupe **system-administrators**, utilisez :

```
# usermod --append -G system-administrators sysadmin
```

Verification steps

- Pour vérifier que les nouveaux groupes ont été ajoutés aux groupes supplémentaires de l'utilisateur **sysadmin**, utiliser :

```
# groups sysadmin
```

Le résultat s'affiche :

```
sysadmin : sysadmin system-administrators
```

17.4. CRÉATION D'UN RÉPERTOIRE DE GROUPE

Dans la configuration du système UPG, vous pouvez appliquer le bit *set-group identification permission* (**setgid**) à un répertoire. Le bit **setgid** simplifie la gestion des projets de groupe qui partagent un répertoire. Lorsque vous appliquez le bit **setgid** à un répertoire, les fichiers créés dans ce répertoire sont automatiquement attribués à un groupe propriétaire du répertoire. Tout utilisateur disposant des droits d'écriture et d'exécution au sein de ce groupe peut désormais créer, modifier et supprimer des fichiers dans le répertoire.

La section suivante décrit comment créer des répertoires de groupe.

Conditions préalables

- **Root** accès

Procédure

1. Créer un répertoire :

```
# mkdir directory-name
```

Remplacez *directory-name* par le nom du répertoire.

2. Créer un groupe :

```
# groupadd group-name
```

Remplacez *group-name* par le nom du groupe.

3. Ajouter des utilisateurs au groupe :

```
# usermod --append -G group-name username
```

Remplacez *group-name* par le nom du groupe et *username* par le nom de l'utilisateur.

4. Associer la propriété de l'utilisateur et du groupe du répertoire au groupe *group-name*:

```
# chgrp group-name directory-name
```

   Remplacez *group-name* par le nom du groupe et *directory-name* par le nom du répertoire.

5. Définissez les autorisations d'écriture pour permettre aux utilisateurs de créer et de modifier des fichiers et des répertoires et définissez le bit **setgid** pour que cette autorisation soit appliquée dans le répertoire *directory-name*:

```
# chmod g rwxs directory-name
```

   Remplacez *directory-name* par le nom du répertoire.

   Désormais, tous les membres du groupe ***group-name*** peuvent créer et modifier des fichiers dans le répertoire ***directory-name*** et les modifier. Les fichiers nouvellement créés conservent la propriété du groupe ***group-name*** groupe.

Verification steps

- Pour vérifier l'exactitude des autorisations définies, utilisez la fonction :

```
# ls -ld directory-name
```

  Remplacez *directory-name* par le nom du répertoire.

  La sortie revient :

```
drwxrwsr-x. 2 root group-name 6 Nov 25 08:45 directory-name
```

CHAPITRE 18. MODIFICATION DES GROUPES D'UTILISATEURS À L'AIDE DE LA LIGNE DE COMMANDE

Un utilisateur appartient à un certain ensemble de groupes qui permettent à une collection logique d'utilisateurs d'avoir un accès similaire aux fichiers et aux dossiers. Vous pouvez modifier les groupes d'utilisateurs primaires et supplémentaires à partir de la ligne de commande pour changer les autorisations de l'utilisateur.

18.1. GROUPES D'UTILISATEURS PRIMAIRES ET COMPLÉMENTAIRES

Un groupe est une entité qui relie plusieurs comptes d'utilisateurs dans un but commun, par exemple pour accorder l'accès à des fichiers particuliers.

Sous Linux, les groupes d'utilisateurs peuvent être primaires ou supplémentaires. Les groupes primaires et supplémentaires ont les propriétés suivantes :

Groupe primaire

- Chaque utilisateur n'a qu'un seul groupe primaire en permanence.
- Vous pouvez modifier le groupe principal de l'utilisateur.

Groupes supplémentaires

- Vous pouvez ajouter un utilisateur existant à un groupe supplémentaire existant pour gérer les utilisateurs ayant les mêmes privilèges de sécurité et d'accès au sein du groupe.
- Les utilisateurs peuvent être membres de zéro ou de plusieurs groupes supplémentaires.

18.2. LISTE DES GROUPES PRIMAIRES ET SUPPLÉMENTAIRES D'UN UTILISATEUR

Vous pouvez dresser la liste des groupes d'utilisateurs pour voir à quels groupes primaires et supplémentaires ils appartiennent.

Procédure

- Affiche les noms du groupe principal et de tout groupe supplémentaire d'un utilisateur :

```
groupes de dollars user-name
```

Remplacez *user-name* par le nom de l'utilisateur. Si vous ne fournissez pas de nom d'utilisateur, la commande affiche l'appartenance au groupe de l'utilisateur actuel. Le premier groupe est le groupe principal, suivi des groupes supplémentaires facultatifs.

Exemple 18.1. Liste des groupes pour l'utilisateur sarah :

```
$ groups sarah
```

Le résultat s'affiche :

```
sarah : sarah wheel developer
```

L'utilisateur **sarah** a un groupe primaire **sarah** et est membre des groupes supplémentaires **wheel** et **developer**.

Exemple 18.2. Liste des groupes pour l'utilisateur marc :

```
$ groups marc
```

Le résultat s'affiche :

```
marc : marc
```

L'utilisateur **marc** n'a qu'un groupe primaire **marc** et aucun groupe supplémentaire.

18.3. MODIFIER LE GROUPE PRINCIPAL D'UN UTILISATEUR

Vous pouvez changer le groupe principal d'un utilisateur existant en un nouveau groupe.

Prérequis :

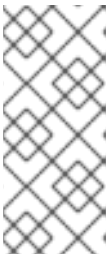
1. **root** access
2. Le nouveau groupe doit exister

Procédure

- Modifier le groupe principal d'un utilisateur :

```
# usermod -g group-name user-name
```

Remplacez *group-name* par le nom du nouveau groupe primaire et *user-name* par le nom de l'utilisateur.



NOTE

Lorsque vous modifiez le groupe principal d'un utilisateur, la commande modifie également automatiquement la propriété de tous les fichiers du répertoire personnel de l'utilisateur en fonction du nouveau groupe principal. Vous devez fixer manuellement la propriété du groupe pour les fichiers situés en dehors du répertoire personnel de l'utilisateur.

Exemple 18.3. Exemple de modification du groupe primaire d'un utilisateur :

Si l'utilisateur **sarah** appartient au groupe primaire **sarah1**, et que vous voulez changer le groupe primaire de l'utilisateur en **sarah2**, utilisez :

```
# usermod -g sarah2 sarah
```

Verification steps

- Vérifiez que vous avez modifié le groupe principal de l'utilisateur :

```
$ groups sarah
```

Le résultat s'affiche :

```
sarah : sarah2
```

18.4. AJOUTER UN UTILISATEUR À UN GROUPE SUPPLÉMENTAIRE À PARTIR DE LA LIGNE DE COMMANDE

Vous pouvez ajouter un utilisateur à un groupe supplémentaire pour gérer les autorisations ou permettre l'accès à certains fichiers ou appareils.

Conditions préalables

- **root** access

Procédure

- Pour ajouter un groupe aux groupes supplémentaires de l'utilisateur, utiliser :

```
# usermod --append -G group-name username
```

Remplacez *group-name* par le nom du groupe et *username* par le nom de l'utilisateur.

Exemple 18.4. Ajouter un utilisateur à un groupe supplémentaire

Pour ajouter l'utilisateur **sysadmin** au groupe **system-administrators**, utilisez :

```
# usermod --append -G system-administrators sysadmin
```

Verification steps

- Pour vérifier que les nouveaux groupes ont été ajoutés aux groupes supplémentaires de l'utilisateur **sysadmin**, utiliser :

```
# groups sysadmin
```

Le résultat s'affiche :

```
sysadmin : sysadmin system-administrators
```

18.5. SUPPRESSION D'UN UTILISATEUR D'UN GROUPE SUPPLÉMENTAIRE

Vous pouvez supprimer un utilisateur existant d'un groupe supplémentaire afin de limiter ses autorisations ou son accès aux fichiers et aux appareils.

Conditions préalables

- **root** access

Procédure

- Supprimer un utilisateur d'un groupe supplémentaire :

```
# gpasswd -d user-name group-name
```

Remplacez *user-name* par le nom de l'utilisateur et *group-name* par le nom du groupe supplémentaire.

Exemple 18.5. Suppression d'un utilisateur d'un groupe supplémentaire

Si l'utilisateur sarah a un groupe primaire **sarah2**, et appartient aux groupes secondaires **wheel** et **developers**, et que vous voulez supprimer cet utilisateur du groupe **developers**, utilisez :

```
# gpasswd -d sarah developers
```

Verification steps

- Vérifiez que vous avez supprimé l'utilisateur sarah du groupe secondaire developers :

```
$ groups sarah
```

Le résultat s'affiche :

```
sarah : sarah2 wheel
```

18.6. MODIFIER TOUS LES GROUPES SUPPLÉMENTAIRES D'UN UTILISATEUR

Vous pouvez modifier la liste des groupes supplémentaires dont l'utilisateur doit rester membre.

Conditions préalables

- **root** access
- Les groupes supplémentaires doivent exister

Procédure

- Remplacer une liste de groupes supplémentaires d'utilisateurs :

```
# usermod -G group-names username
```

Remplacez *group-names* par le nom d'un ou de plusieurs groupes supplémentaires. Pour ajouter l'utilisateur à plusieurs groupes supplémentaires à la fois, séparez les noms des groupes par des virgules sans espace. Par exemple : **wheel,developer**.

Replace *user-name* with the name of the user.

IMPORTANT

Si l'utilisateur est actuellement membre d'un groupe que vous n'avez pas spécifié, la commande supprime l'utilisateur du groupe.

Exemple 18.6. Modifier la liste des groupes supplémentaires d'un utilisateur

Si l'utilisateur **sarah** a un groupe primaire **sarah2**, qu'il appartient au groupe complémentaire **wheel**, et que vous souhaitez qu'il appartienne à trois autres groupes complémentaires **developer**, **sysadmin**, et **security**, utilisez :

```
# usermod -G wheel,developer,sysadmin,security sarah
```

Verification steps

- Vérifiez que la liste des groupes supplémentaires est correcte :

```
# groups sarah
```

Le résultat s'affiche :

```
sarah : sarah2 wheel developer sysadmin security
```

CHAPITRE 19. GESTION DE L'ACCÈS SUDO

Les administrateurs système peuvent accorder l'accès à **sudo** pour permettre aux utilisateurs non root d'exécuter des commandes administratives qui sont normalement réservées à l'utilisateur **root**. Ainsi, les utilisateurs non root peuvent entrer ces commandes sans se connecter au compte utilisateur **root**.

19.1. AUTORISATIONS DES UTILISATEURS DANS SUDOERS

Le fichier **/etc/sudoers** spécifie quels utilisateurs peuvent exécuter quelles commandes à l'aide de la commande **sudo**. Les règles peuvent s'appliquer à des utilisateurs individuels ou à des groupes d'utilisateurs. Vous pouvez également utiliser des alias pour simplifier la définition de règles pour des groupes d'hôtes, de commandes et même d'utilisateurs. Les alias par défaut sont définis dans la première partie du fichier **/etc/sudoers**.

Lorsqu'un utilisateur tente d'utiliser les privilèges de **sudo** pour exécuter une commande qui n'est pas autorisée dans le fichier **/etc/sudoers**, le système enregistre un message contenant ***username* : user NOT in sudoers** dans le journal.

Le fichier par défaut **/etc/sudoers** fournit des informations et des exemples d'autorisations. Vous pouvez activer un exemple de règle spécifique en supprimant le caractère de commentaire **#** au début de la ligne. La section sur les autorisations pertinente pour l'utilisateur est marquée par l'introduction suivante :

```
## Next comes the main part: which users can run what software on
## which machines  (the sudoers file can be shared between multiple
## systems).
```

Vous pouvez utiliser le format suivant pour créer de nouvelles autorisations **sudoers** et pour modifier les autorisations existantes :

```
username hostname=path/to/command
```

Où ?

- *username* est le nom de l'utilisateur ou du groupe, par exemple **user1** ou **%group1**.
- *hostname* est le nom de l'hôte sur lequel la règle s'applique.
- *path/to/command* est le chemin absolu complet de la commande. Vous pouvez également limiter l'utilisateur à l'exécution d'une commande avec des options et des arguments spécifiques en ajoutant ces options après le chemin d'accès à la commande. Si vous ne spécifiez aucune option, l'utilisateur peut utiliser la commande avec toutes les options.

Vous pouvez remplacer n'importe laquelle de ces variables par **ALL** pour appliquer la règle à tous les utilisateurs, hôtes ou commandes.

AVERTISSEMENT

Avec des règles trop permissives, telles que **ALL ALL=(ALL) ALL**, tous les utilisateurs sont en mesure d'exécuter toutes les commandes en tant que tous les utilisateurs sur tous les hôtes. Cela peut entraîner des risques pour la sécurité.

Vous pouvez spécifier les arguments de manière négative en utilisant l'opérateur **!**. Par exemple, utilisez **!root** pour spécifier tous les utilisateurs à l'exception de l'utilisateur **root**. Notez que l'utilisation des listes d'autorisation pour autoriser des utilisateurs, des groupes et des commandes spécifiques est plus sûre que l'utilisation des listes de blocage pour interdire des utilisateurs, des groupes et des commandes spécifiques. En utilisant les listes d'autorisation, vous bloquez également les nouveaux utilisateurs ou groupes non autorisés.

AVERTISSEMENT

Évitez d'utiliser des règles négatives pour les commandes, car les utilisateurs peuvent contourner ces règles en renommant les commandes à l'aide de la commande **alias**.

Le système lit le fichier **/etc/sudoers** du début à la fin. Par conséquent, si le fichier contient plusieurs entrées pour un utilisateur, les entrées sont appliquées dans l'ordre. En cas de valeurs contradictoires, le système utilise la dernière correspondance, même si elle n'est pas la plus spécifique.

Pour ajouter de nouvelles règles à **sudoers**, il est préférable de créer de nouveaux fichiers dans le répertoire **/etc/sudoers.d/** plutôt que de saisir les règles directement dans le fichier **/etc/sudoers**. En effet, le contenu de ce répertoire est préservé lors des mises à jour du système. En outre, il est plus facile de corriger les erreurs dans les fichiers séparés que dans le fichier **/etc/sudoers**. Le système lit les fichiers du répertoire **/etc/sudoers.d** lorsqu'il atteint la ligne suivante dans le fichier **/etc/sudoers**:

```
#includedir /etc/sudoers.d
```

Notez que le signe numérique **#** au début de cette ligne fait partie de la syntaxe et ne signifie pas que la ligne est un commentaire. Les noms des fichiers de ce répertoire ne doivent pas contenir de point **.** et ne doivent pas se terminer par un tilde **~**.

Ressources supplémentaires

- **sudo(8)** et **sudoers(5)** pages de manuel

19.2. ACCORDER L'ACCÈS SUDO À UN UTILISATEUR

Les administrateurs système peuvent accorder l'accès **sudo** pour permettre à des utilisateurs non root d'exécuter des commandes administratives. La commande **sudo** permet aux utilisateurs d'avoir un accès administratif sans utiliser le mot de passe de l'utilisateur **root**.

Lorsque les utilisateurs doivent exécuter une commande administrative, ils peuvent la faire précéder de **sudo**. La commande est alors exécutée comme s'il s'agissait de l'utilisateur **root**.

Il faut tenir compte des limitations suivantes :

- Seuls les utilisateurs répertoriés dans le fichier de configuration **/etc/sudoers** peuvent utiliser la commande **sudo**.
- La commande est exécutée dans le shell de l'utilisateur, et non dans le shell **root**.

Conditions préalables

- **root** access

Procédure

1. En tant que root, ouvrez le fichier **/etc/sudoers**.

```
# visudo
```

   Le fichier **/etc/sudoers** définit les politiques appliquées par la commande **sudo**.

2. Dans le fichier **/etc/sudoers**, recherchez les lignes qui accordent à **sudo** l'accès aux utilisateurs du groupe administratif **wheel**.

```
## Allows people in group wheel to run all commands
%wheel        ALL=(ALL)       ALL
```

3. Assurez-vous que la ligne qui commence par **%wheel** n'est pas précédée du caractère de commentaire **#**.
4. Enregistrez les modifications et quittez l'éditeur.
5. Ajoutez au groupe administratif **wheel** les utilisateurs auxquels vous souhaitez accorder l'accès à **sudo**.

```
# usermod --append -G wheel <username>
```

   Remplacez *<username>* par le nom de l'utilisateur.

Verification steps

- Vérifiez que l'utilisateur est ajouté au groupe administratif **wheel**:

```
# id <username>
uid=5000(<username>) gid=5000(<username>) groups=5000(<username>),10(wheel)
```

Ressources supplémentaires

- **sudo(8)**, **visudo(8)**, et **sudoers(5)** pages de manuel

19.3. PERMETTRE AUX UTILISATEURS NON PRIVILÉGIÉS D'EXÉCUTER CERTAINES COMMANDES

En tant qu'administrateur, vous pouvez autoriser les utilisateurs non privilégiés à entrer certaines commandes sur des postes de travail spécifiques en configurant une stratégie dans le répertoire **/etc/sudoers.d/**.

Par exemple, vous pouvez permettre à l'utilisateur *<example.user>* d'installer des programmes sur la station de travail **host.example.com** en utilisant la commande **dnf** avec les privilèges **sudo**.

Conditions préalables

- Vous devez avoir accès au système à l'adresse **root**.

Procédure

1. En tant que **root**, créez un nouveau répertoire **sudoers.d** sous **/etc/**:

```
# mkdir -p /etc/sudoers.d/
```

2. Créez un nouveau fichier dans le répertoire **/etc/sudoers.d**:

```
# visudo -f /etc/sudoers.d/<example.user>
```

   Le fichier s'ouvre automatiquement.

3. Ajoutez la ligne suivante au fichier **/etc/sudoers.d/*<example.user>*** la ligne suivante :

```
<example.user> <host.example.com> = /usr/bin/dnf
```

   Pour autoriser plusieurs commandes sur le même hôte sur une même ligne, vous pouvez les énumérer en les séparant par une virgule **,** suivie d'un espace.

4. Facultatif : Pour recevoir des notifications par courrier électronique chaque fois que l'utilisateur *<example.user>* tente d'utiliser les privilèges de **sudo**, ajoutez les lignes suivantes au fichier :

```
Defaults    mail_always
Defaults    mailto="<email@example.com>"
```

5. Enregistrez les modifications et quittez l'éditeur.

Vérification

1. Pour vérifier si l'utilisateur *<example.user>* peut exécuter la commande **dnf** avec les privilèges de **sudo**, changez de compte :

```
# su <example.user> -
```

2. Entrez la commande **sudo dnf**:

```
$ sudo dnf
[sudo] password for <example.user>:
```

   Saisissez le mot de passe **sudo** pour l'utilisateur *<example.user>*.

3. Le système affiche la liste des commandes et des options de **dnf**:

```
...
usage: dnf [options] COMMAND
...
```

Si le système renvoie le message d'erreur ***<example.user>* is not in the sudoers file. This incident will be reported** vous n'avez pas créé le fichier pour *<example.user>* dans **/etc/sudoers.d/**.

Si vous recevez le message d'erreur ***<example.user>* is not allowed to run sudo on *<host.example.com>*** vous n'avez pas effectué la configuration correctement. Assurez-vous que vous êtes bien connecté en tant que **root** et que vous avez bien suivi les étapes.

Ressources supplémentaires

- **sudo(8)**, **visudo(8)**, et **sudoers(5)** pages de manuel

CHAPITRE 20. MODIFICATION ET RÉINITIALISATION DU MOT DE PASSE ROOT

Si le mot de passe root existant n'est plus satisfaisant ou a été oublié, vous pouvez le modifier ou le réinitialiser à la fois en tant qu'utilisateur **root** et en tant qu'utilisateur non root.

20.1. MODIFIER LE MOT DE PASSE ROOT EN TANT QU'UTILISATEUR ROOT

Cette section décrit comment utiliser la commande **passwd** pour modifier le mot de passe de **root** en tant qu'utilisateur de **root**.

Conditions préalables

- **Root** accès

Procédure

- Pour modifier le mot de passe de **root**, utilisez

```
# passwd
```

  Vous êtes invité à saisir votre mot de passe actuel avant de pouvoir le modifier.

20.2. MODIFIER OU RÉINITIALISER LE MOT DE PASSE ROOT OUBLIÉ EN TANT QU'UTILISATEUR NON ROOT

Cette section décrit comment utiliser la commande **passwd** pour modifier ou réinitialiser le mot de passe oublié de **root** en tant qu'utilisateur non root.

Conditions préalables

- Vous pouvez vous connecter en tant qu'utilisateur non root.
- Vous êtes membre du groupe administratif **wheel**.

Procédure

- Pour modifier ou réinitialiser le mot de passe **root** en tant qu'utilisateur non root appartenant au groupe **wheel**, utilisez la commande suivante :

```
$ sudo passwd root
```

  Vous êtes invité à saisir votre mot de passe non root actuel avant de pouvoir modifier le mot de passe **root**.

20.3. RÉINITIALISATION DU MOT DE PASSE ROOT AU DÉMARRAGE

Si vous ne pouvez pas vous connecter en tant qu'utilisateur non root ou si vous n'appartenez pas au groupe administratif **wheel**, vous pouvez réinitialiser le mot de passe root au démarrage en basculant dans un environnement spécialisé **chroot jail**.

Procédure

1. Redémarrez le système et, sur l'écran de démarrage de GRUB 2, appuyez sur la touche **e** pour interrompre le processus de démarrage.
   Les paramètres de démarrage du noyau apparaissent.

```
load_video
set gfx_payload=keep
insmod gzio
linux ($root)/vmlinuz-5.14.0-70.22.1.e19_0.x86_64 root=/dev/mapper/rhel-root ro crash\
kernel=auto resume=/dev/mapper/rhel-swap rd.lvm.lv/swap rhgb quiet
initrd ($root)/initramfs-5.14.0-70.22.1.e19_0.x86_64.img $tuned_initrd
```

2. Allez à la fin de la ligne qui commence par **linux**.

```
linux ($root)/vmlinuz-5.14.0-70.22.1.e19_0.x86_64 root=/dev/mapper/rhel-root ro crash\
kernel=auto resume=/dev/mapper/rhel-swap rd.lvm.lv/swap rhgb quiet
```

   Appuyez sur **Ctrl e** pour sauter à la fin de la ligne.

3. Ajouter **rd.break** à la fin de la ligne qui commence par **linux**.

```
linux ($root)/vmlinuz-5.14.0-70.22.1.e19_0.x86_64 root=/dev/mapper/rhel-root ro crash\
kernel=auto resume=/dev/mapper/rhel-swap rd.lvm.lv/swap rhgb quiet rd.break
```

4. Appuyez sur **Ctrl x** pour démarrer le système avec les paramètres modifiés.
   L'invite **switch_root** apparaît.

5. Remonter le système de fichiers en écriture :

```
mount -o remount,rw /sysroot
```

   Le système de fichiers est monté en lecture seule dans le répertoire /**sysroot**. Le fait de remonter le système de fichiers en écriture permet de modifier le mot de passe.

6. Entrez dans l'environnement **chroot**:

```
chroot /sysroot
```

   L'invite **sh-4.4#** apparaît.

7. Réinitialiser le mot de passe **root**:

```
passwd
```

   Suivez les instructions affichées par la ligne de commande pour finaliser la modification du mot de passe **root**.

8. Activer le processus de réétiquetage SELinux au prochain démarrage du système :

```
touch /.autorelabel
```

9. Quitter l'environnement **chroot**:

```
exit
```

10. Quittez l'invite **switch_root**:

```
exit
```

11. Attendez que le processus de réétiquetage SELinux soit terminé. Notez que le réétiquetage d'un disque de grande taille peut prendre beaucoup de temps. Le système redémarre automatiquement lorsque le processus est terminé.

Verification steps

1. Pour vérifier que le mot de passe **root** a bien été modifié, connectez-vous en tant qu'utilisateur normal et ouvrez le terminal.
2. Exécutez l'interpréteur de commandes interactif en tant que root :

```
$ su
```

3. Saisissez votre nouveau mot de passe **root**.
4. Imprime le nom de l'utilisateur associé à l'ID utilisateur effectif actuel :

```
whoami
```

La sortie revient :

```
root
```

CHAPITRE 21. GESTION DES AUTORISATIONS DE FICHIERS

Les autorisations de fichiers contrôlent la capacité des comptes d'utilisateurs et de groupes à visualiser, modifier, accéder et exécuter le contenu des fichiers et des répertoires.

Chaque fichier ou répertoire possède trois niveaux de propriété :

- Propriétaire de l'utilisateur (**u**).
- Propriétaire du groupe (**g**).
- Autres (**o**).

Chaque niveau de propriété peut se voir attribuer les autorisations suivantes :

- Lire (**r**).
- Écrire (**w**).
- Exécuter (**x**).

Notez que l'autorisation d'exécution d'un fichier vous permet d'exécuter ce fichier. Le droit d'exécution d'un répertoire vous permet d'accéder au contenu du répertoire, mais pas de l'exécuter.

Lorsqu'un nouveau fichier ou répertoire est créé, les autorisations par défaut lui sont automatiquement attribuées. Les autorisations par défaut d'un fichier ou d'un répertoire sont basées sur deux facteurs :

- Permission de base.
- Le site *user file-creation mode mask* (**umask**).

21.1. AUTORISATIONS POUR LES FICHIERS DE BASE

Chaque fois qu'un nouveau fichier ou répertoire est créé, une autorisation de base lui est automatiquement attribuée. Les autorisations de base pour un fichier ou un répertoire peuvent être exprimées en valeurs *symbolic* ou *octal*.

Permission	Symbolic value	Octal value
Pas d'autorisation	---	0
Exécuter	--x	1
Écrire	-w-	2
Rédiger et exécuter	-wx	3
Lire	r--	4
Lire et exécuter	r-x	5
Lire et écrire	rw-	6

Lire, écrire, exécuter	rwx	7

L'autorisation de base pour un répertoire est **777** (**drwxrwxrwx**), qui accorde à chacun les autorisations de lecture, d'écriture et d'exécution. Cela signifie que le propriétaire du répertoire, le groupe et d'autres personnes peuvent dresser la liste du contenu du répertoire, créer, supprimer et modifier des éléments dans le répertoire et y descendre.

Notez que les fichiers individuels d'un répertoire peuvent avoir leur propre autorisation, ce qui peut vous empêcher de les modifier, même si vous avez un accès illimité au répertoire.

L'autorisation de base pour un fichier est **666** (**-rw-rw-rw-**), ce qui permet à tout le monde de lire et d'écrire. Cela signifie que le propriétaire du fichier, le groupe et d'autres personnes peuvent lire et modifier le fichier.

Exemple 21.1. Autorisations pour un fichier

Si un fichier a les permissions suivantes :

```
$ ls -l
-rwxrw----. 1 sysadmins sysadmins 2 Mar 2 08:43 file
```

- **-** indique qu'il s'agit d'un fichier.
- **rwx** indique que le propriétaire du fichier a le droit de lire, d'écrire et d'exécuter le fichier.
- **rw-** indique que le groupe a le droit de lire et d'écrire, mais pas d'exécuter le fichier.
- **---** indique que les autres utilisateurs n'ont pas le droit de lire, d'écrire ou d'exécuter le fichier.
- **.** indique que le contexte de sécurité SELinux est défini pour le fichier.

Exemple 21.2. Autorisations pour un répertoire

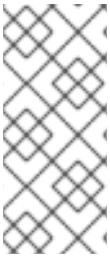
Si un répertoire a les permissions suivantes :

```
$ ls -dl directory
drwxr-----. 1 sysadmins sysadmins 2 Mar 2 08:43 directory
```

- **d** indique qu'il s'agit d'un répertoire.
- **rwx** indique que le propriétaire du répertoire dispose des droits de lecture, d'écriture et d'accès au contenu du répertoire.
  En tant que propriétaire d'un répertoire, vous pouvez dresser la liste des éléments (fichiers, sous-répertoires) qui s'y trouvent, accéder au contenu de ces éléments et les modifier.
- **r-x** indique que le groupe a le droit de lire le contenu du répertoire, mais pas d'écrire - de créer de nouvelles entrées ou de supprimer des fichiers. L'autorisation **x** signifie que vous pouvez également accéder au répertoire à l'aide de la commande **cd**.
- **---** indique que les autres utilisateurs n'ont pas le droit de lire, d'écrire ou d'accéder au contenu du répertoire.

Si vous n'êtes pas propriétaire d'un utilisateur ou d'un groupe de l'annuaire, vous ne pouvez pas dresser la liste des éléments de l'annuaire, ni accéder aux informations relatives à ces éléments, ni les modifier.

- **.** indique que le contexte de sécurité SELinux est défini pour le répertoire.



NOTE

L'autorisation de base qui est automatiquement attribuée à un fichier ou à un répertoire est **not** l'autorisation par défaut du fichier ou du répertoire. Lorsque vous créez un fichier ou un répertoire, l'autorisation de base est modifiée par l'autorisation *umask*. La combinaison de l'autorisation de base et de l'autorisation *umask* crée l'autorisation par défaut pour les fichiers et les répertoires.

21.2. MASQUE DU MODE DE CRÉATION DE FICHIERS UTILISATEUR

Le masque du mode de création de fichiers par l'utilisateur (*umask*) est une variable qui contrôle la manière dont les autorisations sont définies pour les fichiers et les répertoires nouvellement créés. L'adresse *umask* supprime automatiquement les autorisations de la valeur de base afin d'accroître la sécurité globale d'un système Linux. L'adresse *umask* peut être exprimée en valeurs *symbolic* ou *octal*.

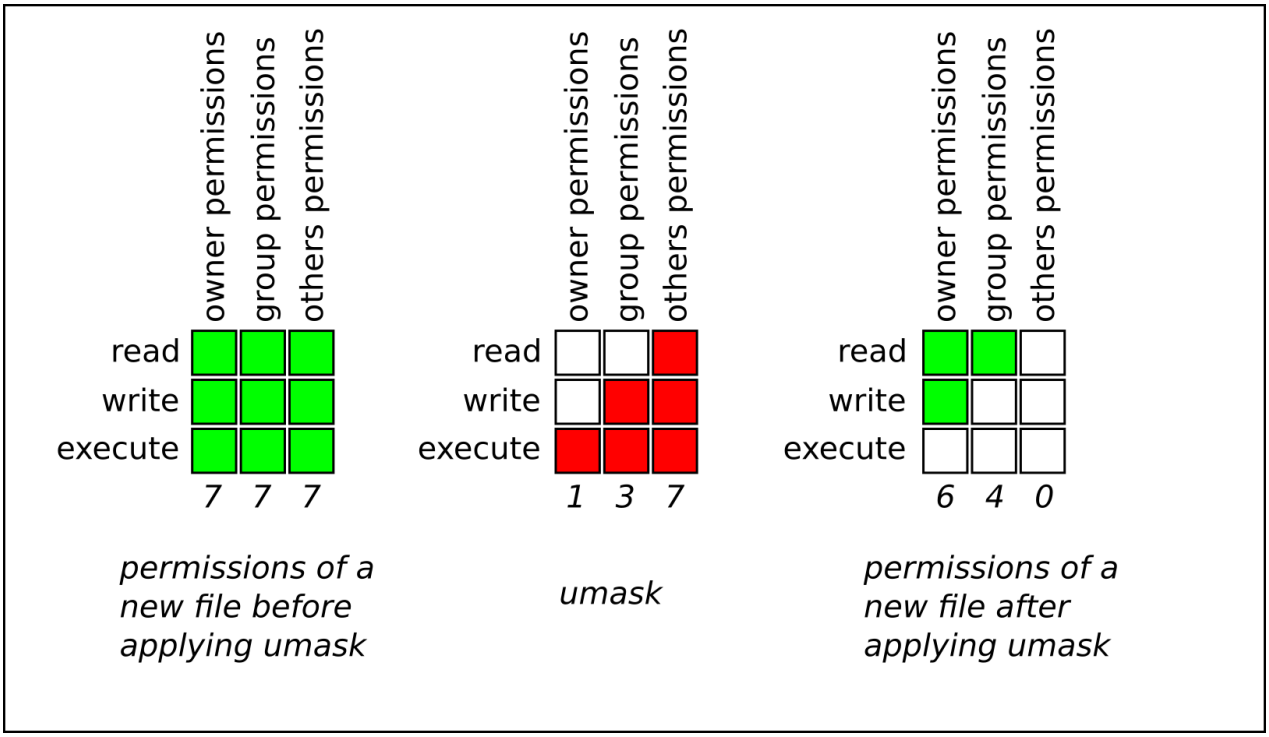
Permission	Symbolic value	Octal value
Lire, écrire et exécuter	rwx	0
Lire et écrire	rw-	1
Lire et exécuter	r-x	2
Lire	r--	3
Rédiger et exécuter	-wx	4
Écrire	-w-	5
Exécuter	--x	6
Aucune autorisation	---	7

La valeur par défaut de *umask* pour un utilisateur standard et pour un utilisateur de **root** est **0022**.

Le premier chiffre de *umask* représente les autorisations spéciales (sticky bit,). Les trois derniers chiffres de *umask* représentent les autorisations qui sont retirées au propriétaire de l'utilisateur (**u**), au propriétaire du groupe (**g**) et aux autres (**o**) respectivement.

Exemple 21.3. Application de l'umask lors de la création d'un fichier

umask L'exemple suivant illustre la manière dont la valeur octale de **0137** est appliquée au fichier dont l'autorisation de base est **777**, afin de créer le fichier dont l'autorisation par défaut est **640**.



21.3. AUTORISATIONS PAR DÉFAUT POUR LES FICHIERS

Les autorisations par défaut sont définies automatiquement pour tous les fichiers et répertoires nouvellement créés. La valeur des autorisations par défaut est déterminée par l'application de *umask* à l'autorisation de base.

Exemple 21.4. Autorisations par défaut pour un répertoire

Lorsqu'un **standard user** ou un **root user** crée un nouveau **directory**, le *umask* est mis à **022** (**rwxr-xr-x**), et les permissions de base pour un répertoire sont mises à **777** (**rwxrwxrwx**). Les autorisations par défaut sont donc fixées à **755** (**rwxr-xr-x**).

	Symbolic value	Octal value
Base permission	rwxrwxrwx	777
Umask	rwxr-xr-x	022
Default permission	rwxr-xr-x	755

Cela signifie que le propriétaire du répertoire peut dresser la liste du contenu du répertoire, créer, supprimer et modifier des éléments dans le répertoire, et descendre dans le répertoire. Le groupe et les autres ne peuvent que lister le contenu du répertoire et y descendre.

Exemple 21.5. Autorisations par défaut pour un fichier

Lorsqu'un **standard user** ou un **root user** crée un nouveau **file**, le *umask* est mis à **022** (**rwxr-xr-x**), et les permissions de base pour un fichier sont mises à **666** (**rw-rw-rw-**). Les autorisations par défaut sont donc fixées à **644** (**-rw-r—r--**).

	Symbolic value	Octal value
Base permission	rw-rw-rw-	666
Umask	rwxr-xr-x	022
Default permission	rw-r-r--	644

Cela signifie que le propriétaire du fichier peut lire et modifier le fichier, tandis que le groupe et les autres ne peuvent que lire le fichier.

NOTE

Pour des raisons de sécurité, les fichiers ordinaires ne peuvent pas avoir de droits d'exécution par défaut, même si l'adresse *umask* est réglée sur **000** (**rwxrwxrwx**). Toutefois, les répertoires peuvent être créés avec des droits d'exécution.

21.4. MODIFICATION DES AUTORISATIONS DE FICHIERS À L'AIDE DE VALEURS SYMBOLIQUES

Vous pouvez utiliser l'utilitaire **chmod** avec des valeurs symboliques (une combinaison de lettres et de signes) pour modifier les autorisations d'un fichier ou d'un répertoire.

Vous pouvez attribuer les *permissions* suivants :

- Lire (**r**)
- Écriture (**w**)
- Exécuter (**x**)

Des autorisations peuvent être attribuées aux sites suivants : *levels of ownership*:

- Propriétaire de l'utilisateur (**u**)
- Propriétaire du groupe (**g**)
- Autre (**o**)
- Tous (**a**)

Pour ajouter ou supprimer des permissions, vous pouvez utiliser la méthode suivante : *signs*:

- pour ajouter les autorisations en plus des autorisations existantes
- **-** pour supprimer les autorisations de l'autorisation existante
- **=** pour supprimer les autorisations existantes et définir explicitement les nouvelles autorisations

Procédure

- Pour modifier les autorisations d'un fichier ou d'un répertoire, utilisez la fonction :

```
$ chmod <level><operation><permission> file-name
```

Remplacer ***<level>*** par le niveau de propriété pour lequel vous souhaitez définir les autorisations. Remplacer ***<operation>*** par l'un des signes. Remplacer ***<permission>*** par les autorisations que vous souhaitez attribuer. Remplacez *file-name* par le nom du fichier ou du répertoire. Par exemple, pour accorder à tout le monde les droits de lecture, d'écriture et d'exécution (**rwx**) **my-script.sh**, utilisez la commande **chmod a=rwx my-script.sh**.

Pour plus de détails, voir les autorisations de fichiers de base .

Verification steps

- Pour voir les permissions d'un fichier particulier, utilisez :

```
$ ls -l file-name
```

Remplacez *file-name* par le nom du fichier.

- Pour voir les permissions d'un répertoire particulier, utilisez :

```
$ ls -dl directory-name
```

Remplacez *directory-name* par le nom du répertoire.

- Pour afficher les autorisations de tous les fichiers d'un répertoire particulier, utilisez la commande suivante :

```
$ ls -l directory-name
```

Remplacez *directory-name* par le nom du répertoire.

Exemple 21.6. Modification des autorisations pour les fichiers et les répertoires

- Pour modifier les autorisations de fichiers pour **my-file.txt** de **-rw-rw-r--** à **-rw------**, utilisez :

1. Afficher les autorisations actuelles pour **my-file.txt**:

```
$ ls -l my-file.txt
-rw-rw-r--. 1 username username 0 Feb 24 17:56 my-file.txt
```

2. Supprimez les autorisations de lecture, d'écriture et d'exécution (**rwx**) du fichier au groupe propriétaire (**g**) et aux autres (**o**) :

```
$ chmod go= my-file.txt
```

Notez que toute autorisation qui n'est pas spécifiée après le signe égal (**=**) est automatiquement interdite.

3. Vérifiez que les autorisations pour **my-file.txt** ont été définies correctement :

```
$ ls -l my-file.txt
-rw-------. 1 username username 0 Feb 24 17:56 my-file.txt
```

- Pour modifier les autorisations de fichiers pour **my-directory** de **drwxrwx---** à **drwxrwxr-x**, utilisez :

  1. Afficher les autorisations actuelles pour **my-directory**:

     ```
     $ ls -dl my-directory
     drwxrwx---. 2 username username 4096 Feb 24 18:12 my-directory
     ```

  2. Ajouter l'accès en lecture et en exécution (**r-x**) pour tous les utilisateurs (**a**) :

     ```
     $ chmod o+rx my-directory
     ```

  3. Vérifiez que les autorisations pour **my-directory** et son contenu ont été définies correctement :

     ```
     $ ls -dl my-directory
     drwxrwxr-x. 2 username username 4096 Feb 24 18:12 my-directory
     ```

21.5. MODIFICATION DES AUTORISATIONS DE FICHIERS À L'AIDE DE VALEURS OCTALES

Vous pouvez utiliser l'utilitaire **chmod** avec des valeurs octales (nombres) pour modifier les autorisations d'un fichier ou d'un répertoire.

Procédure

- Pour modifier les autorisations d'un fichier ou d'un répertoire existant, utilisez la commande suivante :

  ```
  $ chmod octal_value file-name
  ```

  Remplacez *file-name* par le nom du fichier ou du répertoire. Remplacez *octal_value* par une valeur octale. Voir Base file permissions pour plus de détails.

CHAPITRE 22. GESTION DE L'UMASK

Vous pouvez utiliser l'utilitaire **umask** pour afficher, définir ou modifier la valeur actuelle ou par défaut de *umask*.

22.1. AFFICHAGE DE LA VALEUR ACTUELLE DE L'UMASK

Vous pouvez utiliser l'utilitaire **umask** pour afficher la valeur actuelle de *umask* en mode symbolique ou octal.

Procédure

- Pour afficher la valeur actuelle du site *umask* en mode symbolique, utilisez :

```
$ umask -S
```

- Pour afficher la valeur actuelle du site *umask* en mode octal, utilisez :

```
$ umask
```

NOTE

Lorsque vous affichez le *umask* en mode octal, vous pouvez remarquer qu'il est affiché sous la forme d'un nombre à quatre chiffres (**0002** ou **0022**). Le premier chiffre de *umask* représente un bit spécial (bit collant, bit SGID ou bit SUID). Si le premier chiffre est fixé à **0**, le bit spécial n'est pas fixé.

22.2. AFFICHAGE DE L'UMASK PAR DÉFAUT DE BASH

Il existe un certain nombre de shells que vous pouvez utiliser, tels que **bash**, **ksh**, **zsh** et **tcsh**. Ces shells peuvent se comporter comme des shells de connexion ou de non- connexion. Vous pouvez invoquer l'interpréteur de commandes de connexion en ouvrant un terminal natif ou une interface graphique.

Pour déterminer si vous exécutez une commande dans un shell avec ou sans login, utilisez la commande **echo $0**.

Exemple 22.1. Déterminer si vous travaillez dans un shell bash avec ou sans login

- Si la sortie de la commande **echo $0** renvoie **bash**, vous exécutez la commande dans un shell sans login.

```
$ echo $0
bash
```

  La valeur par défaut de *umask* pour le shell non connecté est définie dans le fichier de configuration **/etc/bashrc**.

- Si la sortie de la commande **echo $0** renvoie **-bash**, vous exécutez la commande dans un shell de connexion.

```
# echo $0
-bash
```

La valeur par défaut de *umask* pour le shell de connexion est définie dans le fichier de configuration **/etc/login.defs**.

Procédure

- Pour afficher la valeur par défaut de **bash** *umask* pour l'interpréteur de commandes sans connexion, utilisez la commande suivante

```
$ grep umask /etc/bashrc
```

La sortie revient :

```
# By default, we want umask to get set. This sets it for non-login shell.
      umask 002
      umask 022
```

- Pour afficher la valeur par défaut de **bash** *umask* pour l'interpréteur de commandes de connexion, utilisez la commande suivante :

```
grep "UMASK" /etc/login.defs
```

La sortie revient :

```
# UMASK is also used by useradd(8) and newusers(8) to set the mode for new
UMASK        022
# If HOME_MODE is not set, the value of UMASK is used to create the mode.
```

22.3. DÉFINITION DE L'UMASK À L'AIDE DE VALEURS SYMBOLIQUES

Vous pouvez utiliser l'utilitaire **umask** avec des valeurs symboliques (une combinaison de lettres et de signes) pour définir *umask* pour la session shell en cours

Vous pouvez attribuer les *permissions* suivants :

- Lire (**r**)
- Écriture (**w**)
- Exécuter (**x**)

Des autorisations peuvent être attribuées aux sites suivants : *levels of ownership*:

- Propriétaire de l'utilisateur (**u**)
- Propriétaire du groupe (**g**)
- Autre (**o**)
- Tous (**a**)

Pour ajouter ou supprimer des permissions, vous pouvez utiliser la méthode suivante : *signs*:

- pour ajouter les autorisations en plus des autorisations existantes

- **-** pour supprimer les autorisations de l'autorisation existante
- **=** pour supprimer les autorisations existantes et définir explicitement les nouvelles autorisations

NOTE

Toute autorisation qui n'est pas spécifiée après le signe égal (**=**) est automatiquement interdite.

Procédure

- Pour définir l'adresse *umask* pour la session shell en cours, utilisez la touche

```
$ umask -S <level><operation><permission>
```

Remplacer ***<level>*** par le niveau de propriété pour lequel vous souhaitez définir l'umask. Remplacer ***<operation>*** par l'un des signes. Remplacer ***<permission>*** par les autorisations que vous souhaitez attribuer. Par exemple, pour définir *umask* sur **u=rwx,g=rwx,o=rwx**, utilisez **umask -S a=rwx**.

Pour plus de détails, voir Mode de création de fichiers par l'utilisateur .

NOTE

Le site *umask* n'est valable que pour la session shell en cours.

22.4. DÉFINITION DE L'UMASK À L'AIDE DE VALEURS OCTALES

Vous pouvez utiliser l'utilitaire **umask** avec des valeurs octales (nombres) pour définir *umask* pour la session shell en cours.

Procédure

- Pour définir l'adresse *umask* pour la session shell en cours, utilisez la touche

```
$ umask octal_value
```

Remplacez *octal_value* par une valeur octale. Voir Masque de mode de création de fichier utilisateur pour plus de détails.

NOTE

Le site *umask* n'est valable que pour la session shell en cours.

22.5. MODIFIER L'UMASK PAR DÉFAUT DE L'INTERPRÉTEUR DE COMMANDES SANS LOGIN

Vous pouvez modifier la valeur par défaut de **bash** *umask* pour les utilisateurs standard en modifiant le fichier **/etc/bashrc**.

Conditions préalables

- **root** access

Procédure

1. Comme **root**, ouvrez le fichier **/etc/bashrc** dans l'éditeur.
2. Modifiez les sections suivantes pour définir une nouvelle valeur par défaut **bash** *umask* :

```
if [ $UID -gt 199 ] && [ “id -gn” = “id -un” ]; then
   umask 002
else
   umask 022
fi
```

   Remplacer la valeur octale par défaut de *umask* (**002**) par une autre valeur octale. Voir Masque de mode de création de fichier utilisateur pour plus de détails.

3. Enregistrez les modifications et quittez l'éditeur.

22.6. MODIFIER L'UMASK PAR DÉFAUT DE L'INTERPRÉTEUR DE COMMANDES

Vous pouvez changer la valeur par défaut de **bash** *umask* pour l'utilisateur **root** en modifiant le fichier **/etc/login.defs**.

Conditions préalables

- **root** access

Procédure

1. Comme **root**, ouvrez le fichier **/etc/login.defs** dans l'éditeur.
2. Modifiez les sections suivantes pour définir une nouvelle valeur par défaut **bash** *umask* :

```
# Default initial "umask" value used by login(1) on non-PAM enabled systems.
# Default "umask" value for pam_umask(8) on PAM enabled systems.
# UMASK is also used by useradd(8) and newusers(8) to set the mode for new
# home directories if HOME_MODE is not set.
# 022 is the default value, but 027, or even 077, could be considered
# for increased privacy. There is no One True Answer here: each sysadmin
# must make up their mind.

UMASK           022
```

   Remplacer la valeur octale par défaut de *umask* (**022**) par une autre valeur octale. Voir Masque de mode de création de fichier utilisateur pour plus de détails.

3. Enregistrez les modifications et quittez l'éditeur.

22.7. MODIFIER L'UMASK PAR DÉFAUT POUR UN UTILISATEUR SPÉCIFIQUE

Vous pouvez changer la valeur par défaut de *umask* pour un utilisateur spécifique en modifiant la valeur de **.bashrc** pour cet utilisateur.

Procédure

- Ajouter la ligne qui spécifie la valeur octale de *umask* dans le fichier **.bashrc** pour l'utilisateur en question.

```
$ echo 'umask octal_value' >> /home/username/.bashrc
```

Remplacez *octal_value* par une valeur octale et remplacez *username* par le nom de l'utilisateur. Voir Masque du mode de création de fichier de l'utilisateur pour plus de détails.

22.8. DÉFINITION DES AUTORISATIONS PAR DÉFAUT POUR LES RÉPERTOIRES PERSONNELS NOUVELLEMENT CRÉÉS

Vous pouvez modifier les modes de permission pour les répertoires personnels des utilisateurs nouvellement créés en modifiant le fichier **/etc/login.defs**.

Procédure

1. Comme **root**, ouvrez le fichier **/etc/login.defs** dans l'éditeur.
2. Modifiez la section suivante pour définir une nouvelle valeur par défaut *HOME_MODE*:

```
# HOME_MODE is used by useradd(8) and newusers(8) to set the mode for new
# home directories.
# If HOME_MODE is not set, the value of UMASK is used to create the mode.
HOME_MODE       0700
```

Remplacer la valeur octale par défaut (**0700**) par une autre valeur octale. Le mode sélectionné sera utilisé pour créer les autorisations pour le répertoire personnel.

3. Si *HOME_MODE* est activé, enregistrez les modifications et quittez l'éditeur.
4. Si *HOME_MODE* n'est pas défini, modifiez *UMASK* pour définir le mode des répertoires personnels nouvellement créés :

```
# Default initial "umask" value used by login(1) on non-PAM enabled systems.
# Default "umask" value for pam_umask(8) on PAM enabled systems.
# UMASK is also used by useradd(8) and newusers(8) to set the mode for new
# home directories if HOME_MODE is not set.
# 022 is the default value, but 027, or even 077, could be considered
# for increased privacy. There is no One True Answer here: each sysadmin
# must make up their mind.

UMASK           022
```

Remplacer la valeur octale par défaut (**022**) par une autre valeur octale. Voir Masque du mode de création de fichier utilisateur pour plus de détails.

5. Enregistrez les modifications et quittez l'éditeur.

CHAPITRE 23. ENREGISTREMENT DES REQUÊTES DNS À L'AIDE DE DNSTAP DANS RHEL

En tant qu'administrateur réseau, vous pouvez enregistrer les détails du système de noms de domaine (DNS) pour analyser les schémas de trafic DNS, surveiller les performances du serveur DNS et résoudre les problèmes DNS. Si vous souhaitez disposer d'un moyen avancé de surveiller et d'enregistrer les détails des requêtes de noms entrantes, utilisez l'interface **dnstap** qui enregistre les messages envoyés par le service **named**. Vous pouvez capturer et enregistrer les requêtes DNS pour collecter des informations sur les sites web ou les adresses IP.

Conditions préalables

- Mettre à jour les paquets **BIND** vers la version **bind-9.16.15-3** ou ultérieure, qui contient l'interface **dnstap**.

AVERTISSEMENT

Si une version de **BIND** est déjà installée et fonctionne, l'ajout d'une nouvelle version de **BIND** écrasera la version existante.

Procédure

1. Activez **dnstap** et le fichier cible en modifiant le fichier **/etc/named.conf** dans le bloc **options**:

```
options
{
# …

dnstap { all; }; # Configure filter
dnstap-output file "/var/named/data/dnstap.bin" versions 2;

# …
};
# end of options
```

2. Pour spécifier les types de trafic DNS que vous souhaitez enregistrer, ajoutez des filtres **dnstap** au bloc **dnstap** dans le fichier **/etc/named.conf**. Vous pouvez utiliser les filtres suivants :

   - **auth** - Réponse ou réponse d'une zone faisant autorité.
   - **client** - Requête ou réponse interne du client.
   - **forwarder** - Requête transmise ou réponse de sa part.
   - **resolver** - Requête ou réponse de résolution itérative.
   - **update** - Demandes de mise à jour dynamique de la zone.
   - **all** - N'importe laquelle des options ci-dessus.

- **query** ou **response** - Si vous ne spécifiez pas de mot-clé **query** ou **response**, **dnstap** enregistre les deux.

NOTE

Le filtre **dnstap** contient plusieurs définitions délimitées par un **;** dans le bloc **dnstap {}** avec la syntaxe suivante : **dnstap { (all | auth | client | forwarder | resolver | update) [(query | response)]; ... };**

3. Pour personnaliser le comportement de l'utilitaire **dnstap** sur les paquets enregistrés, modifiez l'option **dnstap-output** en fournissant des paramètres supplémentaires, comme suit :

   - **size** (illimité | <size>) - Active le renouvellement automatique du fichier **dnstap** lorsque sa taille atteint la limite spécifiée.

   - **versions** (illimité | <integer>) - Spécifiez le nombre de fichiers roulés automatiquement à conserver.

   - **suffix** (incrément | horodatage) - Choisissez la convention de nommage pour les fichiers déployés. Par défaut, l'incrément commence par **.0**. Vous pouvez également utiliser l'horodatage UNIX en définissant la valeur **timestamp**.
     L'exemple suivant demande uniquement les réponses de **auth**, les requêtes de **client** et à la fois les requêtes et les réponses de la dynamique **updates**:

     Example:

     ```
     dnstap {auth response; client query; update;};
     ```

4. Pour appliquer vos modifications, redémarrez le service **named**:

   ```
   # systemctl restart named.service
   ```

5. Configurer un déploiement périodique pour les journaux actifs
   Dans l'exemple suivant, le planificateur **cron** exécute le contenu du script édité par l'utilisateur une fois par jour. L'option **roll** avec la valeur **3** spécifie que **dnstap** peut créer jusqu'à trois fichiers journaux de sauvegarde. La valeur **3** remplace le paramètre **version** de la variable **dnstap-output** et limite le nombre de fichiers journaux de sauvegarde à trois. En outre, le fichier journal binaire est déplacé dans un autre répertoire et renommé, et il n'atteint jamais le suffixe **.2**, même si trois fichiers journaux de sauvegarde existent déjà. Vous pouvez ignorer cette étape si le roulement automatique des journaux binaires en fonction de la taille limite est suffisant.

   Example:

   ```
   sudoedit /etc/cron.daily/dnstap

   #!/bin/sh
   rndc dnstap -roll 3
   mv /var/named/data/dnstap.bin.1 /var/log/named/dnstap/dnstap-$(date -I).bin

   # use dnstap-read to analyze saved logs
   sudo chmod a+x /etc/cron.daily/dnstap
   ```

6. L'utilitaire **dnstap-read** permet de traiter et d'analyser les journaux dans un format lisible par l'homme :

Dans l'exemple suivant, l'utilitaire **dnstap-read** imprime la sortie au format de fichier **YAML**.

Example:

```
dnstap-read -y [file-name]
```

CHAPITRE 24. GESTION DE LA LISTE DE CONTRÔLE D'ACCÈS

Chaque fichier et répertoire ne peut avoir qu'un seul propriétaire d'utilisateur et un seul propriétaire de groupe à la fois. Si vous souhaitez accorder à un utilisateur des autorisations d'accès à des fichiers ou répertoires spécifiques appartenant à un autre utilisateur ou groupe, tout en gardant d'autres fichiers et répertoires privés, vous pouvez utiliser les listes de contrôle d'accès (ACL) de Linux.

24.1. AFFICHAGE DE LA LISTE DE CONTRÔLE D'ACCÈS ACTUELLE

Vous pouvez utiliser l'utilitaire **getfacl** pour afficher l'ACL actuel.

Procédure

- Pour afficher l'ACL actuelle d'un fichier ou d'un répertoire particulier, utilisez la commande suivante :

```
getfacl file-name
```

  Remplacez *file-name* par le nom du fichier ou du répertoire.

24.2. CONFIGURATION DE LA LISTE DE CONTRÔLE D'ACCÈS

Vous pouvez utiliser l'utilitaire **setfacl** pour définir l'ACL d'un fichier ou d'un répertoire.

Conditions préalables

- **root** l'accès.

Procédure

- Pour définir l'ACL d'un fichier ou d'un répertoire, utilisez la commande suivante :

```
# setfacl -m u :usernamesymbolic_value file-name
```

Remplacez *username* par le nom de l'utilisateur, *symbolic_value* par une valeur symbolique et *file-name* par le nom du fichier ou du répertoire. Pour plus d'informations, voir la page de manuel **setfacl**.

Exemple 24.1. Modifier les autorisations pour un projet de groupe

L'exemple suivant décrit comment modifier les autorisations pour le fichier **group-project** appartenant à l'utilisateur **root** qui appartient au groupe **root** afin que ce fichier soit :

- N'est pas exécutable par quiconque.
- L'utilisateur **andrew** a les permissions de **rw-**.
- L'utilisateur **susan** a les permissions de **---**.
- Les autres utilisateurs ont les autorisations **r--**.

Procédure

```
# setfacl -m u:andrew:rw- group-project
# setfacl -m u:susan:--- group-project
```

Verification steps

- Pour vérifier que l'utilisateur **andrew** dispose de l'autorisation **rw-**, que l'utilisateur **susan** dispose de l'autorisation **---** et que les autres utilisateurs disposent de l'autorisation **r--**, utilisez :

```
$ getfacl group-project
```

La sortie revient :

```
# file: group-project
# owner: root
# group: root
user:andrew:rw-
user:susan:---
group::r--
mask::rw-
other::r--
```

CHAPITRE 25. UTILISATION DE LA SUITE CHRONY POUR CONFIGURER NTP

Un chronométrage précis est important pour plusieurs raisons dans le domaine des technologies de l'information. Dans les réseaux, par exemple, des horodatages précis sont nécessaires dans les paquets et les journaux. Dans les systèmes Linux, le protocole **NTP** est mis en œuvre par un démon fonctionnant dans l'espace utilisateur.

Le démon de l'espace utilisateur met à jour l'horloge système exécutée dans le noyau. L'horloge système peut garder l'heure en utilisant différentes sources d'horloge. Habituellement, c'est la source *Time Stamp Counter* (**TSC**) qui est utilisée. Le TSC est un registre du processeur qui compte le nombre de cycles depuis sa dernière remise à zéro. Il est très rapide, a une haute résolution et ne subit aucune interruption.

À partir de Red Hat Enterprise Linux 8, le protocole **NTP** est implémenté par le démon **chronyd**, disponible dans les dépôts dans le paquetage **chrony**.

Les sections suivantes décrivent comment utiliser la suite **chrony** pour configurer NTP.

25.1. INTRODUCTION À LA SUITE CHRONOLOGIQUE

chrony est une implémentation de **Network Time Protocol (NTP)**. Vous pouvez utiliser **chrony**:

- Pour synchroniser l'horloge du système avec les serveurs **NTP**
- Pour synchroniser l'horloge du système avec une horloge de référence, par exemple un récepteur GPS
- Pour synchroniser l'horloge du système avec une entrée manuelle de l'heure
- En tant que serveur ou homologue **NTPv4(RFC 5905)** pour fournir un service horaire à d'autres ordinateurs du réseau

chrony fonctionne bien dans un large éventail de conditions, y compris les connexions réseau intermittentes, les réseaux fortement encombrés, les changements de température (les horloges d'ordinateur ordinaires sont sensibles à la température), et les systèmes qui ne fonctionnent pas en continu, ou qui fonctionnent sur une machine virtuelle.

La précision typique entre deux machines synchronisées sur l'internet est de quelques millisecondes, et pour les machines sur un réseau local de quelques dizaines de microsecondes. L'horodatage matériel ou une horloge de référence matérielle peut améliorer la précision entre deux machines synchronisées à un niveau inférieur à la microseconde.

chrony se compose de **chronyd**, un démon qui s'exécute dans l'espace utilisateur, et de **chronyc**un programme en ligne de commande qui peut être utilisé pour surveiller les performances de **chronyd** et pour modifier divers paramètres de fonctionnement lorsqu'il est en cours d'exécution.

Le démon **chronychronyd** , peut être surveillé et contrôlé par l'utilitaire de ligne de commande **chronyc**. Cet utilitaire fournit une invite de commande qui permet d'entrer un certain nombre de commandes pour interroger l'état actuel de **chronyd** et apporter des modifications à sa configuration. Par défaut, **chronyd** n'accepte que les commandes provenant d'une instance locale de **chronyc**mais il peut être configuré pour accepter également des commandes de surveillance provenant d'hôtes distants. L'accès à distance doit être limité.

25.2. UTILISATION DE CHRONYC POUR CONTRÔLER CHRONYD

Cette section décrit comment contrôler **chronyd** à l'aide de l'utilitaire de ligne de commande **chronyc** à l'aide de l'utilitaire de ligne de commande.

Procédure

1. Pour apporter des modifications à l'instance locale de **chronyd** à l'aide de l'utilitaire de ligne de commande **chronyc** en mode interactif, entrez la commande suivante sous **root**:

```
# chronyc
```

chronyc doit être exécuté en tant que **root** si certaines des commandes restreintes doivent être utilisées.

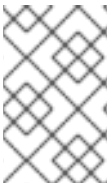
L'invite de commande **chronyc** l'invite de commande s'affiche comme suit :

```
chronyc>
```

2. Pour obtenir la liste de toutes les commandes, tapez **help**.

3. L'utilitaire peut également être invoqué en mode de commande non interactive s'il est appelé en même temps qu'une commande comme suit :

```
chronyc command
```



NOTE

Les modifications effectuées à l'aide de **chronyc** ne sont pas permanentes, elles seront perdues après un redémarrage de **chronyd**. Pour des changements permanents, modifiez /**etc**/**chrony.conf**.

CHAPITRE 26. UTILISATION DE CHRONY

Les sections suivantes décrivent comment installer, démarrer et arrêter **chronyd**, et comment vérifier si **chrony** est synchronisé. Les sections décrivent également comment ajuster manuellement l'horloge du système.

26.1. GESTION DE LA CHRONOLOGIE

La procédure suivante décrit comment installer, démarrer, arrêter et vérifier l'état de **chronyd**.

Procédure

1. La suite **chrony** est installée par défaut sur Red Hat Enterprise Linux. Pour vous en assurer, exécutez la commande suivante à l'adresse **root**:

```
# dnf install chrony
```

   L'emplacement par défaut du **chrony** est **/usr/sbin/chronyd**. L'utilitaire de ligne de commande sera installé à l'adresse **/usr/bin/chronyc**.

2. Pour vérifier l'état de **chronyd**, lancez la commande suivante :

```
$ systemctl status chronyd
chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled)
   Active: active (running) since Wed 2013-06-12 22:23:16 CEST; 11h ago
```

3. Pour démarrer **chronyd**, lancez la commande suivante en tant que **root**:

```
# systemctl start chronyd
```

   Pour que **chronyd** démarre automatiquement au démarrage du système, lancez la commande suivante en tant que **root**:

```
# systemctl enable chronyd
```

4. Pour arrêter **chronyd**, lancez la commande suivante en tant que **root**:

```
# systemctl stop chronyd
```

   Pour éviter que **chronyd** ne démarre automatiquement au démarrage du système, exécutez la commande suivante en tant que **root**:

```
# systemctl disable chronyd
```

26.2. VÉRIFICATION DE LA SYNCHRONISATION DU CHŒUR

La procédure suivante décrit comment vérifier si **chrony** est synchronisé à l'aide des commandes **tracking**, **sources**, et **sourcestats**.

Procédure

1. Pour vérifier le **chrony** le suivi, lancez la commande suivante :

```
$ chronyc tracking
Reference ID    : CB00710F (foo.example.net)
Stratum         : 3
Ref time (UTC)  : Fri Jan 27 09:49:17 2017
System time     :  0.000006523 seconds slow of NTP time
Last offset     : -0.000006747 seconds
RMS offset      : 0.000035822 seconds
Frequency       : 3.225 ppm slow
Residual freq   : 0.000 ppm
Skew            : 0.129 ppm
Root delay      : 0.013639022 seconds
Root dispersion : 0.001100737 seconds
Update interval : 64.2 seconds
Leap status     : Normal
```

2. La commande sources affiche des informations sur les sources de temps actuelles auxquelles **chronyd** accède. Pour vérifier **chrony** sources, lancez la commande suivante :

```
$ chronyc sources
 210 Number of sources = 3
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
====
#* GPS0                          0   4   377    11   -479ns[ -621ns] /-  134ns
^? a.b.c                        2   6   377    23   -923us[ -924us] +/-   43ms
^ d.e.f                         1   6   377    21  -2629us[-2619us] +/-   86ms
```

L'argument optionnel -v peut être spécifié, ce qui signifie verbeux. Dans ce cas, des lignes de légende supplémentaires sont affichées pour rappeler la signification des colonnes.

3. La commande **sourcestats** affiche des informations sur le taux de dérive et le processus d'estimation du décalage pour chacune des sources en cours d'examen par **chronyd**. Pour vérifier les **chrony** les statistiques sur les sources, lancez la commande suivante :

```
$ chronyc sourcestats
210 Number of sources = 1
Name/IP Address            NP  NR  Span  Frequency  Freq Skew  Offset  Std Dev
===============================================================================
====
abc.def.ghi                11   5   46m     -0.001      0.045      1us    25us
```

L'argument facultatif **-v** peut être spécifié, ce qui signifie verbeux. Dans ce cas, des lignes de légende supplémentaires sont affichées pour rappeler la signification des colonnes.

Ressources supplémentaires

- **chronyc(1)** page de manuel

26.3. RÉGLAGE MANUEL DE L'HORLOGE SYSTÈME

La procédure suivante décrit comment régler manuellement l'horloge du système.

Procédure

Procédure

1. Pour passer immédiatement à l'horloge système, en contournant les ajustements en cours par pivotement, lancez la commande suivante à l'adresse **root**:

```
# chronyc maketep
```

Si la directive **rtcfile** est utilisée, l'horloge en temps réel ne doit pas être ajustée manuellement. Des ajustements aléatoires interféreraient avec le besoin de **chrony**le besoin de mesurer la vitesse à laquelle l'horloge en temps réel dérive.

26.4. DÉSACTIVATION D'UN SCRIPT CHRONY DISPATCHER

Le script **chrony** dispatcher gère l'état en ligne et hors ligne des serveurs NTP. En tant qu'administrateur système, vous pouvez désactiver le script dispatcher pour que **chronyd** interroge constamment les serveurs.

Si vous activez NetworkManager sur votre système pour gérer la configuration du réseau, le NetworkManager exécute le script **chrony** dispatcher lors des opérations de reconfiguration, d'arrêt ou de démarrage des interfaces. Cependant, si vous configurez certaines interfaces ou routes en dehors de NetworkManager, vous pouvez rencontrer la situation suivante :

1. Le script du répartiteur peut s'exécuter alors qu'il n'existe aucune route vers les serveurs NTP, ce qui entraîne le passage des serveurs NTP à l'état hors ligne.
2. Si vous établissez la route ultérieurement, le script ne s'exécute pas à nouveau par défaut et les serveurs NTP restent hors ligne.

Pour que **chronyd** puisse se synchroniser avec vos serveurs NTP, qui ont des interfaces gérées séparément, désactivez le script dispatcher.

Conditions préalables

- Vous avez installé NetworkManager sur votre système et l'avez activé.
- Accès à la racine

Procédure

1. Pour désactiver le script de distribution **chrony**, créez un lien symbolique vers **/dev/null**:

```
# ln -s /dev/null /etc/NetworkManager/dispatcher.d/20-chrony-onoffline
```

NOTE

Après cette modification, le NetworkManager ne peut pas exécuter le script du répartiteur et les serveurs NTP restent toujours en ligne.

26.5. MISE EN PLACE DE CHRONY POUR UN SYSTÈME DANS UN RÉSEAU ISOLÉ

Pour un réseau qui n'est jamais connecté à l'internet, un ordinateur est sélectionné pour être le serveur de temps primaire. Les autres ordinateurs sont soit des clients directs du serveur, soit des clients de clients. Sur le serveur, le fichier de dérive doit être défini manuellement avec le taux moyen de dérive de

l'horloge du système. Si le serveur est redémarré, il obtient l'heure des systèmes environnants et calcule une moyenne pour régler son horloge système. Ensuite, il recommence à appliquer des ajustements basés sur le fichier de dérive. Le fichier de dérive est mis à jour automatiquement lorsque la commande **settime** est utilisée.

La procédure suivante décrit comment configurer **chrony** pour un système dans un réseau isolé.

Procédure

1. Sur le système sélectionné comme serveur, à l'aide d'un éditeur de texte fonctionnant sous **root**, modifiez **/etc/chrony.conf** comme suit :

```
driftfile /var/lib/chrony/drift
commandkey 1
keyfile /etc/chrony.keys
initstepslew 10 client1 client3 client6
local stratum 8
manual
allow 192.0.2.0
```

   Où **192.0.2.0** est l'adresse du réseau ou du sous-réseau à partir duquel les clients sont autorisés à se connecter.

2. Sur les systèmes sélectionnés pour être des clients directs du serveur, à l'aide d'un éditeur de texte fonctionnant sous **root**, modifiez le fichier **/etc/chrony.conf** comme suit :

```
server ntp1.example.net
driftfile /var/lib/chrony/drift
logdir /var/log/chrony
log measurements statistics tracking
keyfile /etc/chrony.keys
commandkey 24
local stratum 10
initstepslew 20 ntp1.example.net
allow 192.0.2.123
```

   Où **192.0.2.123** est l'adresse du serveur et **ntp1.example.net** est le nom d'hôte du serveur. Les clients ayant cette configuration se resynchroniseront avec le serveur s'il redémarre.

Sur les systèmes clients qui ne doivent pas être des clients directs du serveur, le fichier **/etc/chrony.conf** doit être identique, à l'exception des directives **local** et **allow** qui doivent être omises.

Dans un réseau isolé, vous pouvez également utiliser la directive **local** qui active un mode de référence local, ce qui permet à **chronyd** fonctionnant comme un serveur **NTP** d'apparaître synchronisé avec le temps réel, même s'il n'a jamais été synchronisé ou si la dernière mise à jour de l'horloge a eu lieu il y a longtemps.

Pour permettre à plusieurs serveurs du réseau d'utiliser la même configuration locale et d'être synchronisés entre eux, sans perturber les clients qui interrogent plus d'un serveur, utilisez l'option **orphan** de la directive **local** qui active le mode orphelin. Chaque serveur doit être configuré pour interroger tous les autres serveurs avec **local**. Cela garantit que seul le serveur ayant le plus petit ID de référence a la référence locale active et que les autres serveurs sont synchronisés avec lui. Lorsque le serveur tombe en panne, un autre prend le relais.

26.6. CONFIGURATION DE L'ACCÈS À LA SURVEILLANCE À DISTANCE

chronyc peut accéder à **chronyd** de deux manières :

- Protocole Internet, IPv4 ou IPv6.
- Socket de domaine Unix, accessible localement par l'utilisateur **root** ou **chrony**.

Par défaut, **chronyc** se connecte au socket du domaine Unix. Le chemin par défaut est **/var/run/chrony/chronyd.sock**. Si cette connexion échoue, ce qui peut se produire par exemple lorsque **chronyc** s'exécute sous un utilisateur non root, **chronyc** essaie de se connecter à 127.0.0.1 puis à ::1.

Seules les commandes de surveillance suivantes, qui n'affectent pas le comportement de **chronyd**, sont autorisées à partir du réseau :

- activité
- liste des manuels
- rtcdata
- lissage
- sources
- statistiques sur les sources d'approvisionnement
- suivi
- waitsync

L'ensemble des hôtes à partir desquels **chronyd** accepte ces commandes peut être configuré avec la directive **cmdallow** dans le fichier de configuration de **chronyd**, ou avec la commande **cmdallow** dans le fichier de configuration de **chronyc**. Par défaut, les commandes ne sont acceptées qu'à partir de localhost (127.0.0.1 ou ::1).

Toutes les autres commandes ne sont autorisées qu'à travers le socket du domaine Unix. Lorsqu'elle est envoyée sur le réseau, **chronyd** répond par une erreur **Not authorised**, même si elle provient de localhost.

La procédure suivante décrit comment accéder à chronyd à distance à l'aide de la commande **chronyc**.

Procédure

1. Autorisez l'accès à partir d'adresses IPv4 et IPv6 en ajoutant ce qui suit au fichier **/etc/chrony.conf**:

   ```
   bindcmdaddress 0.0.0.0
   ```

   ou

   ```
   bindcmdaddress : :
   ```

2. Autoriser les commandes provenant d'une adresse IP, d'un réseau ou d'un sous-réseau distant en utilisant la directive **cmdallow**.
   Ajoutez le contenu suivant au fichier **/etc/chrony.conf**:

   ```
   cmdallow 192.168.1.0/24
   ```

–

3. Ouvrez le port 323 dans le pare-feu pour vous connecter à partir d'un système distant :

```
# firewall-cmd --zone=public --add-port=323/udp
```

En option, vous pouvez ouvrir le port 323 de manière permanente à l'aide de l'option **--permanent**:

```
# firewall-cmd --permanent --zone=public --add-port=323/udp
```

4. Si vous avez ouvert le port 323 de manière permanente, rechargez la configuration du pare-feu :

```
firewall-cmd --reload
```

Ressources supplémentaires

- **chrony.conf(5)** page de manuel

26.7. GESTION DE LA SYNCHRONISATION HORAIRE À L'AIDE DES RÔLES SYSTÈME RHEL

Vous pouvez gérer la synchronisation de l'heure sur plusieurs machines cibles à l'aide du rôle **timesync**. Le rôle **timesync** installe et configure une implémentation NTP ou PTP pour fonctionner en tant que client NTP ou PTP afin de synchroniser l'horloge du système.

AVERTISSEMENT

Le rôle **timesync** remplace la configuration du service fournisseur donné ou détecté sur l'hôte géré. Les paramètres précédents sont perdus, même s'ils ne sont pas spécifiés dans les variables du rôle. Le seul paramètre préservé est le choix du fournisseur si la variable **timesync_ntp_provider** n'est pas définie.

L'exemple suivant montre comment appliquer le rôle **timesync** dans une situation où il n'y a qu'un seul pool de serveurs.

Exemple 26.1. Exemple de playbook appliquant le rôle timesync à un seul pool de serveurs

```
---
- hosts: timesync-test
  vars:
    timesync_ntp_servers:
      - hostname: 2.rhel.pool.ntp.org
        pool: yes
        iburst: yes
  roles:
    - rhel-system-roles.timesync
```

Pour une référence détaillée sur les variables de rôle **timesync**, installez le paquetage **rhel-system-roles** et consultez les fichiers **README.md** ou **README.html** dans le répertoire **/usr/share/doc/rhel-system-roles/timesync**.

Ressources supplémentaires

- Préparation d'un nœud de contrôle et de nœuds gérés à l'utilisation des rôles système RHEL

26.8. RESSOURCES SUPPLÉMENTAIRES

- **chronyc(1)** page de manuel
- **chronyd(8)** page de manuel
- Questions fréquemment posées

CHAPITRE 27. CHRONY AVEC HORODATAGE HW

L'horodatage matériel est une fonction prise en charge par certains contrôleurs d'interface réseau (NIC) qui fournit un horodatage précis des paquets entrants et sortants. **NTP** L'horodatage est généralement créé par le noyau et l'horloge du système **chronyd** avec l'utilisation de l'horloge système. Cependant, lorsque l'horodatage matériel est activé, la carte d'interface réseau utilise sa propre horloge pour générer les horodatages lorsque les paquets entrent ou sortent de la couche de liaison ou de la couche physique. Lorsqu'il est utilisé avec **NTP**, l'horodatage matériel peut améliorer de manière significative la précision de la synchronisation. Pour une précision optimale, les serveurs **NTP** et les clients **NTP** doivent utiliser l'horodatage matériel. Dans des conditions idéales, une précision inférieure à la microseconde est possible.

Un autre protocole de synchronisation temporelle utilisant l'horodatage matériel est **PTP**.

Contrairement à **NTP**, **PTP** s'appuie sur l'assistance des commutateurs et des routeurs du réseau. Si vous souhaitez obtenir la meilleure précision de synchronisation possible, utilisez **PTP** sur les réseaux dotés de commutateurs et de routeurs prenant en charge **PTP**, et préférez **NTP** sur les réseaux dépourvus de tels commutateurs et routeurs.

Les sections suivantes décrivent comment :

- Vérifier la prise en charge de l'horodatage matériel
- Activer l'horodatage matériel
- Configurer l'intervalle d'interrogation du client
- Activer le mode entrelacé
- Configurer le serveur pour un grand nombre de clients
- Vérifier l'horodatage du matériel
- Configurer le pont PTP-NTP

27.1. VÉRIFICATION DE LA PRISE EN CHARGE DE L'HORODATAGE MATÉRIEL

Pour vérifier que l'horodatage matériel avec **NTP** est supporté par une interface, utilisez la commande **ethtool -T**. Une interface peut être utilisée pour l'horodatage matériel avec **NTP** si **ethtool** liste les capacités **SOF_TIMESTAMPING_TX_HARDWARE** et **SOF_TIMESTAMPING_TX_SOFTWARE** ainsi que le mode de filtrage **HWTSTAMP_FILTER_ALL**.

Exemple 27.1. Vérification de la prise en charge de l'horodatage matériel sur une interface spécifique

```
# ethtool -T eth0
```

Sortie :

```
Timestamping parameters for eth0:
Capabilities:
        hardware-transmit     (SOF_TIMESTAMPING_TX_HARDWARE)
        software-transmit     (SOF_TIMESTAMPING_TX_SOFTWARE)
        hardware-receive      (SOF_TIMESTAMPING_RX_HARDWARE)
```

```
        software-receive      (SOF_TIMESTAMPING_RX_SOFTWARE)
        software-system-clock (SOF_TIMESTAMPING_SOFTWARE)
        hardware-raw-clock    (SOF_TIMESTAMPING_RAW_HARDWARE)
PTP Hardware Clock: 0
Hardware Transmit Timestamp Modes:
        off                   (HWTSTAMP_TX_OFF)
        on                    (HWTSTAMP_TX_ON)
Hardware Receive Filter Modes:
        none                  (HWTSTAMP_FILTER_NONE)
        all                   (HWTSTAMP_FILTER_ALL)
        ptpv1-l4-sync         (HWTSTAMP_FILTER_PTP_V1_L4_SYNC)
        ptpv1-l4-delay-req    (HWTSTAMP_FILTER_PTP_V1_L4_DELAY_REQ)
        ptpv2-l4-sync         (HWTSTAMP_FILTER_PTP_V2_L4_SYNC)
        ptpv2-l4-delay-req    (HWTSTAMP_FILTER_PTP_V2_L4_DELAY_REQ)
        ptpv2-l2-sync         (HWTSTAMP_FILTER_PTP_V2_L2_SYNC)
        ptpv2-l2-delay-req    (HWTSTAMP_FILTER_PTP_V2_L2_DELAY_REQ)
        ptpv2-event           (HWTSTAMP_FILTER_PTP_V2_EVENT)
        ptpv2-sync            (HWTSTAMP_FILTER_PTP_V2_SYNC)
        ptpv2-delay-req       (HWTSTAMP_FILTER_PTP_V2_DELAY_REQ)
```

27.2. ACTIVATION DE L'HORODATAGE MATÉRIEL

Pour activer l'horodatage matériel, utilisez la directive **hwtimestamp** dans le fichier **/etc/chrony.conf**. La directive peut spécifier une seule interface, ou un caractère générique peut être utilisé pour activer l'horodatage matériel sur toutes les interfaces qui le supportent. Utilisez le caractère générique dans le cas où aucune autre application, telle que **ptp4l** du paquetage **linuxptp**, n'utilise l'horodatage matériel sur une interface. Plusieurs directives **hwtimestamp** sont autorisées dans le fichier de configuration de chrony.

Exemple 27.2. Activation de l'horodatage matériel en utilisant la directive hwtimestamp

```
hwtimestamp eth0
hwtimestamp eth1
hwtimestamp *
```

27.3. CONFIGURATION DE L'INTERVALLE D'INTERROGATION DU CLIENT

La plage par défaut d'un intervalle d'interrogation (64-1024 secondes) est recommandée pour les serveurs sur Internet. Pour les serveurs locaux et l'horodatage matériel, un intervalle d'interrogation plus court doit être configuré afin de minimiser le décalage de l'horloge système.

La directive suivante dans **/etc/chrony.conf** spécifie un serveur **NTP** local utilisant un intervalle d'interrogation d'une seconde :

```
server ntp.local minpoll 0 maxpoll 0
```

27.4. ACTIVATION DU MODE ENTRELACÉ

NTP les serveurs qui ne sont pas des dispositifs matériels **NTP**, mais plutôt des ordinateurs à usage

général exécutant une implémentation logicielle de **NTP**, telle que **chrony**n'obtiendront un horodatage de transmission matérielle qu'après avoir envoyé un paquet. Ce comportement empêche le serveur de sauvegarder l'horodatage dans le paquet auquel il correspond. Pour permettre aux clients **NTP** de recevoir des horodatages de transmission générés après la transmission, configurez les clients pour qu'ils utilisent le mode entrelacé **NTP** en ajoutant l'option **xleave** à la directive serveur dans **/etc/chrony.conf**:

```
server ntp.local minpoll 0 maxpoll 0 xleave
```

27.5. CONFIGURATION DU SERVEUR POUR UN GRAND NOMBRE DE CLIENTS

La configuration par défaut du serveur permet à quelques milliers de clients au maximum d'utiliser le mode entrelacé simultanément. Pour configurer le serveur pour un plus grand nombre de clients, augmentez la directive **clientloglimit** dans **/etc/chrony.conf**. Cette directive spécifie la taille maximale de la mémoire allouée à l'enregistrement des accès des clients sur le serveur :

```
limite du nombre de clients 100000000
```

27.6. VÉRIFICATION DE L'HORODATAGE DU MATÉRIEL

Pour vérifier que l'interface a bien activé l'horodatage matériel, consultez le journal du système. Le journal devrait contenir un message provenant de **chronyd** pour chaque interface dont l'horodatage matériel a été activé avec succès.

Exemple 27.3. Messages du journal pour les interfaces dont l'horodatage matériel est activé

```
chronyd[4081]: Enabled HW timestamping on eth0
chronyd[4081]: Enabled HW timestamping on eth1
```

Lorsque **chronyd** est configuré comme un client ou un homologue de **NTP**, la commande **chronyc ntpdata** peut indiquer les modes d'horodatage de transmission et de réception ainsi que le mode entrelacé pour chaque source **NTP**:

Exemple 27.4. Rapport sur l'horodatage de l'émission, de la réception et le mode entrelacé pour chaque source NTP

```
# chronyc ntpdata
```

Sortie :

```
Remote address  : 203.0.113.15 (CB00710F)
Remote port     : 123
Local address   : 203.0.113.74 (CB00714A)
Leap status     : Normal
Version         : 4
Mode            : Server
Stratum         : 1
Poll interval   : 0 (1 seconds)
Precision       : -24 (0.000000060 seconds)
```

```
Root delay      : 0.000015 seconds
Root dispersion : 0.000015 seconds
Reference ID    : 47505300 (GPS)
Reference time  : Wed May 03 13:47:45 2017
Offset          : -0.000000134 seconds
Peer delay      : 0.000005396 seconds
Peer dispersion : 0.000002329 seconds
Response time   : 0.000152073 seconds
Jitter asymmetry: +0.00
NTP tests       : 111 111 1111
Interleaved     : Yes
Authenticated   : No
TX timestamping : Hardware
RX timestamping : Hardware
Total TX        : 27
Total RX        : 27
Total valid RX  : 27
```

Exemple 27.5. Rapport sur la stabilité des mesures NTP

```
# chronyc sourcestats
```

Lorsque l'horodatage matériel est activé, la stabilité des mesures de **NTP** devrait être de l'ordre de quelques dizaines ou centaines de nanosecondes, dans des conditions de charge normales. Cette stabilité est indiquée dans la colonne **Std Dev** de la sortie de la commande **chronyc sourcestats**:

Sortie :

```
210 Number of sources = 1
Name/IP Address            NP  NR  Span  Frequency  Freq Skew  Offset  Std Dev
ntp.local                  12   7    11     +0.000      0.019     +0ns    49ns
```

27.7. CONFIGURATION DU PONT PTP-NTP

Si un serveur de temps primaire Precision Time Protocol (**PTP**) très précis est disponible dans un réseau qui ne dispose pas de commutateurs ou de routeurs prenant en charge **PTP**, un ordinateur peut être dédié au fonctionnement d'un client **PTP** et d'un serveur **NTP** de strate 1. Cet ordinateur doit disposer de deux interfaces réseau ou plus et être proche du serveur de temps primaire ou avoir une connexion directe avec lui. Cela garantira une synchronisation très précise dans le réseau.

Configurer les **ptp4l** et **phc2sys** des paquets **linuxptp** afin d'utiliser une interface pour synchroniser l'horloge du système à l'aide de **PTP**.

Configurez **chronyd** pour qu'il fournisse l'heure du système à l'aide de l'autre interface :

Exemple 27.6. Configuration de chronyd pour fournir l'heure système à l'aide de l'autre interface

```
bindaddress 203.0.113.74
hwtimestamp eth1
local stratum 1
```

CHAPITRE 28. APERÇU DE LA SÉCURITÉ TEMPORELLE DU RÉSEAU (NTS) DANS CHRONY

Network Time Security (NTS) est un mécanisme d'authentification pour le protocole NTP (Network Time Protocol), conçu pour s'adapter à un nombre important de clients. Il vérifie que les paquets reçus des machines serveurs ne sont pas altérés lorsqu'ils sont transmis à la machine cliente. Network Time Security (NTS) comprend un protocole d'établissement de clés (NTS-KE) qui crée automatiquement les clés de cryptage utilisées entre le serveur et ses clients.

28.1. ACTIVATION DE LA SÉCURITÉ TEMPORELLE DU RÉSEAU (NTS) DANS LE FICHIER DE CONFIGURATION DU CLIENT

Par défaut, Network Time Security (NTS) n'est pas activé. Vous pouvez l'activer sur le site **/etc/chrony.conf**. Pour ce faire, procédez comme suit :

Conditions préalables

- Serveur avec support NTS

Procédure

Dans le fichier de configuration du client :

1. Spécifiez le serveur avec l'option **nts** en plus de l'option recommandée **iburst**.

```
For example:
server time.example.com iburst nts
server nts.netnod.se iburst nts
server ptbtime1.ptb.de iburst nts
```

2. Pour éviter de répéter la session Network Time Security-Key Establishment (NTS-KE) lors du démarrage du système, ajoutez la ligne suivante à **chrony.conf**, si elle n'est pas présente :

```
ntsdumpdir /var/lib/chrony
```

3. Pour désactiver la synchronisation avec les serveurs NTP (Network Time Protocol) fournis par **DHCP**, commentez ou supprimez la ligne suivante dans **chrony.conf**, si elle est présente :

```
sourcedir /run/chrony-dhcp
```

4. Enregistrez vos modifications.

5. Redémarrez le service **chronyd**:

```
systemctl restart chronyd
```

Vérification

- Vérifiez si les clés **NTS** ont été établies avec succès :

```
# chronyc -N authdata
```

```
Name/IP address  Mode KeyID Type KLen Last Atmp  NAK Cook CLen
==========================================================================
time.example.com  NTS     1   15  256  33m    0    0    8  100
nts.sth1.ntp.se   NTS     1   15  256  33m    0    0    8  100
nts.sth2.ntp.se   NTS     1   15  256  33m    0    0    8  100
```

Les valeurs de **KeyID**, **Type** et **KLen** doivent être différentes de zéro. Si la valeur est nulle, vérifiez dans le journal du système s'il y a des messages d'erreur provenant de **chronyd**.

- Vérifiez que le client effectue des mesures NTP :

```
# chronyc -N sources

MS Name/IP address Stratum Poll Reach LastRx Last sample
===============================================================
time.example.com  3       6   377    45   +355us[ +375us] +/-   11ms
nts.sth1.ntp.se   1       6   377    44   +237us[ +237us] +/-   23ms
nts.sth2.ntp.se   1       6   377    44   -170us[ -170us] +/-   22ms
```

La colonne **Reach** doit avoir une valeur non nulle, idéalement 377. Si la valeur atteint rarement ou jamais 377, cela indique que des requêtes ou des réponses NTP se perdent dans le réseau.

Ressources supplémentaires

- **chrony.conf(5)** page de manuel

28.2. ACTIVATION DE LA SÉCURITÉ TEMPORELLE DU RÉSEAU (NTS) SUR LE SERVEUR

Si vous utilisez votre propre serveur NTP (Network Time Protocol), vous pouvez activer le support NTS (Network Time Security) du serveur pour permettre à ses clients de se synchroniser en toute sécurité.

Si le serveur NTP est un client d'autres serveurs, c'est-à-dire s'il n'est pas un serveur de strate 1, il doit utiliser NTS ou une clé symétrique pour sa synchronisation.

Conditions préalables

- Clé privée du serveur au format **PEM**
- Certificat du serveur avec les certificats intermédiaires requis au format **PEM**

Procédure

1. Indiquez la clé privée et le fichier de certificat dans le champ **chrony.conf**

```
For example:
ntsserverkey /etc/pki/tls/private/foo.example.net.key
ntsservercert /etc/pki/tls/certs/foo.example.net.crt
```

2. Assurez-vous que les fichiers de clés et de certificats sont lisibles par l'utilisateur du système chrony, en définissant la propriété du groupe.

```
For example:
chown :chrony /etc/pki/tls/*/foo.example.net.*
```

3. Assurez-vous que la directive **ntsdumpdir /var/lib/chrony** est présente dans le fichier **chrony.conf**.

4. Redémarrez le service **chronyd**:

```
systemctl restart chronyd
```

IMPORTANT

Si le serveur est équipé d'un pare-feu, il doit autoriser les ports **UDP 123** et **TCP 4460** pour NTP et Network Time Security-Key Establishment (NTS-KE).

Vérification

- Effectuez un test rapide à partir d'une machine cliente à l'aide de la commande suivante :

```
$ chronyd -Q -t 3 'server

foo.example.net iburst nts maxsamples 1'
2021-09-15T13:45:26Z chronyd version 4.1 starting (+CMDMON +NTP +REFCLOCK +RTC
+PRIVDROP +SCFILTER +SIGND +ASYNCDNS +NTS +SECHASH +IPV6 +DEBUG)
2021-09-15T13:45:26Z Disabled control of system clock
2021-09-15T13:45:28Z System clock wrong by 0.002205 seconds (ignored)
2021-09-15T13:45:28Z chronyd exiting
```

Le message **System clock wrong** indique que le serveur NTP accepte les connexions NTS-KE et répond avec des messages NTP protégés par NTS.

- Vérifiez les connexions NTS-KE et les paquets NTP authentifiés observés sur le serveur :

```
# chronyc serverstats

NTP packets received       : 7
NTP packets dropped        : 0
Command packets received   : 22
Command packets dropped    : 0
Client log records dropped : 0
NTS-KE connections accepted: 1
NTS-KE connections dropped : 0
Authenticated NTP packets: 7
```

Si la valeur des champs **NTS-KE connections accepted** et **Authenticated NTP packets** est différente de zéro, cela signifie qu'au moins un client a pu se connecter au port NTS-KE et envoyer une requête NTP authentifiée.

CHAPITRE 29. UTILISER DES COMMUNICATIONS SÉCURISÉES ENTRE DEUX SYSTÈMES AVEC OPENSSH

SSH (Secure Shell) est un protocole qui assure des communications sécurisées entre deux systèmes à l'aide d'une architecture client-serveur et permet aux utilisateurs de se connecter à distance aux systèmes hôtes des serveurs. Contrairement à d'autres protocoles de communication à distance, tels que FTP ou Telnet, SSH crypte la session de connexion, ce qui empêche les intrus de collecter des mots de passe non cryptés à partir de la connexion.

Red Hat Enterprise Linux inclut les paquetages de base **OpenSSH**: le paquetage général **openssh**, le paquetage **openssh-server** et le paquetage **openssh-clients**. Notez que les paquets **OpenSSH** nécessitent le paquetage **OpenSSL openssl-libs** , qui installe plusieurs bibliothèques cryptographiques importantes permettant à **OpenSSH** de fournir des communications cryptées.

29.1. SSH ET OPENSSH

SSH (Secure Shell) est un programme permettant de se connecter à une machine distante et d'y exécuter des commandes. Le protocole SSH fournit des communications cryptées et sécurisées entre deux hôtes non fiables sur un réseau non sécurisé. Vous pouvez également transférer des connexions X11 et des ports TCP/IP arbitraires sur le canal sécurisé.

Le protocole SSH atténue les menaces de sécurité, telles que l'interception des communications entre deux systèmes et l'usurpation d'identité d'un hôte particulier, lorsque vous l'utilisez pour l'ouverture d'une session shell à distance ou la copie de fichiers. En effet, le client et le serveur SSH utilisent des signatures numériques pour vérifier leur identité. En outre, toutes les communications entre les systèmes client et serveur sont cryptées.

Une clé d'hôte authentifie les hôtes dans le protocole SSH. Les clés d'hôte sont des clés cryptographiques générées automatiquement lors de la première installation d'OpenSSH ou lors du premier démarrage de l'hôte.

OpenSSH est une implémentation du protocole SSH supporté par Linux, UNIX et d'autres systèmes d'exploitation similaires. Il comprend les fichiers de base nécessaires au client et au serveur OpenSSH. La suite OpenSSH se compose des outils suivants dans l'espace utilisateur :

- **ssh** est un programme de connexion à distance (client SSH).
- **sshd** est un démon SSH OpenSSH.
- **scp** est un programme sécurisé de copie de fichiers à distance.
- **sftp** est un programme de transfert de fichiers sécurisé.
- **ssh-agent** est un agent d'authentification pour la mise en cache des clés privées.
- **ssh-add** ajoute des identités de clés privées à **ssh-agent**.
- **ssh-keygen** génère, gère et convertit les clés d'authentification pour **ssh**.
- **ssh-copy-id** est un script qui ajoute les clés publiques locales au fichier **authorized_keys** d'un serveur SSH distant.
- **ssh-keyscan** rassemble les clés publiques d'hôte SSH.

NOTE

Dans RHEL 9, le protocole de copie sécurisée (SCP) est remplacé par le protocole de transfert de fichiers SSH (SFTP) par défaut. Cela s'explique par le fait que SCP a déjà causé des problèmes de sécurité, par exemple CVE-2020-15778.

Si SFTP n'est pas disponible ou incompatible dans votre scénario, vous pouvez utiliser l'option **-O** pour forcer l'utilisation du protocole SCP/RCP d'origine.

Pour plus d'informations, consultez l'article sur la dépréciation du protocole SCP d'OpenSSH dans Red Hat Enterprise Linux 9 .

Il existe actuellement deux versions de SSH : la version 1 et la version 2, plus récente. La suite OpenSSH de RHEL ne prend en charge que la version 2 de SSH. Elle dispose d'un algorithme d'échange de clés amélioré qui n'est pas vulnérable aux exploits connus dans la version 1.

OpenSSH, l'un des principaux sous-systèmes cryptographiques de RHEL, utilise des politiques cryptographiques à l'échelle du système. Cela garantit que les suites de chiffrement et les algorithmes cryptographiques faibles sont désactivés dans la configuration par défaut. Pour modifier la politique, l'administrateur doit soit utiliser la commande **update-crypto-policies** pour ajuster les paramètres, soit se retirer manuellement des politiques de chiffrement à l'échelle du système.

La suite OpenSSH utilise deux ensembles de fichiers de configuration : un pour les programmes clients (c'est-à-dire **ssh**, **scp**, et **sftp**), et un autre pour le serveur (le démon **sshd**).

Les informations relatives à la configuration SSH de l'ensemble du système sont stockées dans le répertoire **/etc/ssh/**. Les informations de configuration SSH spécifiques à l'utilisateur sont stockées dans le répertoire **~/.ssh/**, dans le répertoire personnel de l'utilisateur. Pour une liste détaillée des fichiers de configuration OpenSSH, voir la section **FILES** dans la page de manuel **sshd(8)**.

Ressources supplémentaires

- Pages de manuel répertoriées à l'aide de la commande **man -k ssh**
- Utilisation de politiques cryptographiques à l'échelle du système

29.2. CONFIGURATION ET DÉMARRAGE D'UN SERVEUR OPENSSH

Utilisez la procédure suivante pour une configuration de base qui peut être nécessaire pour votre environnement et pour démarrer un serveur OpenSSH. Notez qu'après l'installation par défaut de RHEL, le démon **sshd** est déjà lancé et les clés d'hôte du serveur sont automatiquement créées.

Conditions préalables

- Le paquet **openssh-server** est installé.

Procédure

1. Démarrer le démon **sshd** dans la session en cours et le configurer pour qu'il démarre automatiquement au moment du démarrage :

```
# systemctl start sshd
# systemctl enable sshd
```

2. Pour spécifier des adresses différentes des adresses par défaut **0.0.0.0** (IPv4) ou **::** (IPv6) pour

la directive **ListenAddress** dans le fichier de configuration **/etc/ssh/sshd_config** et pour utiliser une configuration réseau dynamique plus lente, ajoutez la dépendance de l'unité cible **network-online.target** au fichier d'unité **sshd.service**. Pour ce faire, créez le fichier **/etc/systemd/system/sshd.service.d/local.conf** avec le contenu suivant :

```
[Unit]
Wants=network-online.target
After=network-online.target
```

3. Vérifiez que les paramètres du serveur OpenSSH dans le fichier de configuration **/etc/ssh/sshd_config** répondent aux exigences de votre scénario.

4. Vous pouvez également modifier le message de bienvenue que votre serveur OpenSSH affiche avant qu'un client ne s'authentifie en éditant le fichier **/etc/issue**, par exemple :

```
Welcome to ssh-server.example.com
Warning: By accessing this server, you agree to the referenced terms and conditions.
```

Assurez-vous que l'option **Banner** n'est pas commentée dans **/etc/ssh/sshd_config** et que sa valeur contient **/etc/issue**:

```
# less /etc/ssh/sshd_config | grep Banner
Banner /etc/issue
```

Notez que pour modifier le message affiché après une connexion réussie, vous devez éditer le fichier **/etc/motd** sur le serveur. Voir la page de manuel **pam_motd** pour plus d'informations.

5. Rechargez la configuration de **systemd** et redémarrez **sshd** pour appliquer les changements :

```
# systemctl daemon-reload
# systemctl restart sshd
```

Vérification

1. Vérifiez que le démon **sshd** est en cours d'exécution :

```
# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2019-11-18 14:59:58 CET; 6min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1149 (sshd)
    Tasks: 1 (limit: 11491)
   Memory: 1.9M
   CGroup: /system.slice/sshd.service
           └─1149 /usr/sbin/sshd -D -oCiphers=aes128-ctr,aes256-ctr,aes128-cbc,aes256-cbc -
oMACs=hmac-sha2-256,>

Nov 18 14:59:58 ssh-server-example.com systemd[1]: Starting OpenSSH server daemon...
Nov 18 14:59:58 ssh-server-example.com sshd[1149]: Server listening on 0.0.0.0 port 22.
Nov 18 14:59:58 ssh-server-example.com sshd[1149]: Server listening on :: port 22.
Nov 18 14:59:58 ssh-server-example.com systemd[1]: Started OpenSSH server daemon.
```

2. Connectez-vous au serveur SSH avec un client SSH.

```
# ssh user@ssh-server-example.com
ECDSA key fingerprint is SHA256:dXbaS0RG/UzlTTku8GtXSz0S1++lPegSy31v3L/FAEc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ssh-server-example.com' (ECDSA) to the list of known hosts.

user@ssh-server-example.com's password:
```

Ressources supplémentaires

- **sshd(8)** et **sshd_config(5)**.

29.3. CONFIGURATION D'UN SERVEUR OPENSSH POUR L'AUTHENTIFICATION PAR CLÉ

Pour améliorer la sécurité du système, appliquez l'authentification par clé en désactivant l'authentification par mot de passe sur votre serveur OpenSSH.

Conditions préalables

- Le paquet **openssh-server** est installé.
- Le démon **sshd** est en cours d'exécution sur le serveur.

Procédure

1. Ouvrez la configuration de **/etc/ssh/sshd_config** dans un éditeur de texte, par exemple :

```
# vi /etc/ssh/sshd_config
```

2. Remplacer l'option **PasswordAuthentication** par **no**:

```
PasswordAuthentication no
```

   Sur un système autre qu'une nouvelle installation par défaut, vérifiez que **PubkeyAuthentication no** n'a pas été défini et que la directive **KbdInteractiveAuthentication** est définie sur **no**. Si vous êtes connecté à distance, sans utiliser la console ou l'accès hors bande, testez le processus de connexion par clé avant de désactiver l'authentification par mot de passe.

3. Pour utiliser l'authentification par clé avec les répertoires personnels montés sur NFS, activez le booléen SELinux **use_nfs_home_dirs**:

```
# setsebool -P use_nfs_home_dirs 1
```

4. Rechargez le démon **sshd** pour appliquer les modifications :

```
# systemctl reload sshd
```

Ressources supplémentaires

- **sshd(8)**, **sshd_config(5)** et **setsebool(8)**.

29.4. GÉNÉRER DES PAIRES DE CLÉS SSH

Cette procédure permet de générer une paire de clés SSH sur un système local et de copier la clé publique générée sur un serveur OpenSSH. Si le serveur est configuré en conséquence, vous pouvez vous connecter au serveur OpenSSH sans fournir de mot de passe.

IMPORTANT

Si vous effectuez les étapes suivantes en tant que **root**, seul **root** pourra utiliser les clés.

Procédure

1. Pour générer une paire de clés ECDSA pour la version 2 du protocole SSH :

```
$ ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/joesec/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/joesec/.ssh/id_ecdsa.
Your public key has been saved in /home/joesec/.ssh/id_ecdsa.pub.
The key fingerprint is:
SHA256:Q/x+qms4j7PCQ0qFd09iZEFHA+SqwBKRNaU72oZfaCI
joesec@localhost.example.com
The key's randomart image is:
+---[ECDSA 256]---+
|.oo..o=++        |
|.. o .oo .       |
|. .. o. o        |
|....o.+...       |
|o.oo.o +S .      |
|.=.+.   .o       |
|E.*+.  .  . .    |
|.=..+ +..  o     |
|  .  oo*+o.      |
+----[SHA256]-----+
```

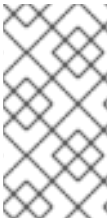
   Vous pouvez également générer une paire de clés RSA en utilisant l'option **-t rsa** avec la commande **ssh-keygen** ou une paire de clés Ed25519 en entrant la commande **ssh-keygen -t ed25519**.

2. Pour copier la clé publique sur une machine distante :

```
$ ssh-copy-id joesec@ssh-server-example.com
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
joesec@ssh-server-example.com's password:
...
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'joesec@ssh-server-example.com'" and check to make sure that only the key(s) you wanted were added.
```

Si vous n'utilisez pas le programme **ssh-agent** dans votre session, la commande précédente copie la clé publique **~/.ssh/id*.pub** la plus récemment modifiée si elle n'est pas encore installée. Pour spécifier un autre fichier de clé publique ou pour donner la priorité aux clés contenues dans les fichiers par rapport aux clés mises en mémoire par **ssh-agent**, utilisez la commande **ssh-copy-id** avec l'option **-i**.



NOTE

Si vous réinstallez votre système et souhaitez conserver les paires de clés générées précédemment, sauvegardez le répertoire **~/.ssh/**. Après la réinstallation, copiez-le dans votre répertoire personnel. Vous pouvez faire cela pour tous les utilisateurs de votre système, y compris **root**.

Vérification

1. Connectez-vous au serveur OpenSSH sans fournir de mot de passe :

```
$ ssh joesec@ssh-server-example.com
Welcome message.
...
Last login: Mon Nov 18 18:28:42 2019 from ::1
```

Ressources supplémentaires

- **ssh-keygen(1)** et **ssh-copy-id(1)**.

29.5. UTILISATION DE CLÉS SSH STOCKÉES SUR UNE CARTE À PUCE

Red Hat Enterprise Linux vous permet d'utiliser les clés RSA et ECDSA stockées sur une carte à puce sur les clients OpenSSH. Utilisez cette procédure pour activer l'authentification à l'aide d'une carte à puce au lieu d'un mot de passe.

Conditions préalables

- Côté client, le paquet **opensc** est installé et le service **pcscd** est en cours d'exécution.

Procédure

1. Dresser la liste de toutes les clés fournies par le module PKCS #11 d'OpenSC, y compris leurs URI PKCS #11, et enregistrer le résultat dans le fichier *keys.pub*:

```
$ ssh-keygen -D pkcs11: > keys.pub
$ ssh-keygen -D pkcs11:
ssh-rsa AAAAB3NzaC1yc2E...KKZMzcQZzx
pkcs11:id=%02;object=SIGN%20pubkey;token=SSH%20key;manufacturer=piv_II?module-
path=/usr/lib64/pkcs11/opensc-pkcs11.so
ecdsa-sha2-nistp256 AAA...J0hkYnnsM=
pkcs11:id=%01;object=PIV%20AUTH%20pubkey;token=SSH%20key;manufacturer=piv_II?
module-path=/usr/lib64/pkcs11/opensc-pkcs11.so
```

2. Pour permettre l'authentification à l'aide d'une carte à puce sur un serveur distant (*example.com*), transférez la clé publique sur le serveur distant. Utilisez la commande **ssh-copy-id** avec *keys.pub* créé à l'étape précédente :

```
$ ssh-copy-id -f -i keys.pub username@example.com
```

3. Pour vous connecter à *example.com* à l'aide de la clé ECDSA issue de la commande **ssh-keygen -D** à l'étape 1, vous pouvez utiliser uniquement un sous-ensemble de l'URI, qui fait référence de manière unique à votre clé, par exemple :

```
$ ssh -i "pkcs11:id=%01?module-path=/usr/lib64/pkcs11/opensc-pkcs11.so" example.com
Enter PIN for 'SSH key':
[example.com] $
```

4. Vous pouvez utiliser la même chaîne URI dans le fichier **~/.ssh/config** pour rendre la configuration permanente :

```
$ cat ~/.ssh/config
IdentityFile "pkcs11:id=%01?module-path=/usr/lib64/pkcs11/opensc-pkcs11.so"
$ ssh example.com
Enter PIN for 'SSH key':
[example.com] $
```

Comme OpenSSH utilise le wrapper **p11-kit-proxy** et que le module OpenSC PKCS #11 est enregistré dans le kit PKCS#11, vous pouvez simplifier les commandes précédentes :

```
$ ssh -i "pkcs11:id=%01" example.com
Enter PIN for 'SSH key':
[example.com] $
```

Si vous omettez la partie **id=** d'un URI PKCS #11, OpenSSH charge toutes les clés disponibles dans le module proxy. Cela peut réduire la quantité de données à saisir :

```
$ ssh -i pkcs11: example.com
Enter PIN for 'SSH key':
[example.com] $
```

Ressources supplémentaires

- Fedora 28 : Meilleur support des cartes à puce dans OpenSSH
- **p11-kit(8)**, **opensc.conf(5)**, **pcscd(8)**, **ssh(1)**, et **ssh-keygen(1)** pages de manuel

29.6. RENDRE OPENSSH PLUS SÛR

Les conseils suivants vous aideront à renforcer la sécurité lors de l'utilisation d'OpenSSH. Notez que les modifications apportées au fichier de configuration d'OpenSSH **/etc/ssh/sshd_config** nécessitent le rechargement du démon **sshd** pour être prises en compte :

```
# systemctl reload sshd
```

IMPORTANT

La majorité des modifications apportées à la configuration du renforcement de la sécurité réduisent la compatibilité avec les clients qui ne prennent pas en charge les algorithmes ou les suites de chiffrement les plus récents.

Désactivation des protocoles de connexion non sécurisés

- Pour que SSH soit vraiment efficace, il faut empêcher l'utilisation de protocoles de connexion non sécurisés qui sont remplacés par la suite OpenSSH. Sinon, le mot de passe d'un utilisateur peut être protégé par SSH pendant une session et être capturé plus tard lors d'une connexion par Telnet. Pour cette raison, envisagez de désactiver les protocoles non sécurisés, tels que telnet, rsh, rlogin et ftp.

Activation de l'authentification par clé et désactivation de l'authentification par mot de passe

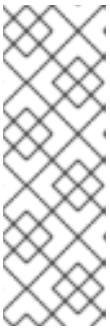
- Le fait de désactiver les mots de passe pour l'authentification et de n'autoriser que les paires de clés réduit la surface d'attaque et peut également faire gagner du temps aux utilisateurs. Sur les clients, générez des paires de clés à l'aide de l'outil **ssh-keygen** et utilisez l'utilitaire **ssh-copy-id** pour copier les clés publiques des clients sur le serveur OpenSSH. Pour désactiver l'authentification par mot de passe sur votre serveur OpenSSH, modifiez **/etc/ssh/sshd_config** et remplacez l'option **PasswordAuthentication** par **no**:

```
PasswordAuthentication no
```

Types de clés

- Bien que la commande **ssh-keygen** génère par défaut une paire de clés RSA, vous pouvez lui demander de générer des clés ECDSA ou Ed25519 en utilisant l'option **-t**. L'ECDSA (Elliptic Curve Digital Signature Algorithm) offre de meilleures performances que le RSA à puissance de clé symétrique équivalente. Il génère également des clés plus courtes. L'algorithme de clé publique Ed25519 est une implémentation des courbes d'Edwards torsadées qui est plus sûre et plus rapide que RSA, DSA et ECDSA.
  OpenSSH crée automatiquement les clés d'hôte RSA, ECDSA et Ed25519 du serveur si elles sont manquantes. Pour configurer la création de clés hôte dans RHEL, utilisez le service instancié **sshd-keygen@.service**. Par exemple, pour désactiver la création automatique du type de clé RSA :

```
# systemctl mask sshd-keygen@rsa.service
```



NOTE

Dans les images où **cloud-init** est activé, les unités **ssh-keygen** sont automatiquement désactivées. En effet, le service **ssh-keygen template** peut interférer avec l'outil **cloud-init** et causer des problèmes avec la génération des clés de l'hôte. Pour éviter ces problèmes, le fichier de configuration drop-in **etc/systemd/system/sshd-keygen@.service.d/disable-sshd-keygen-if-cloud-init-active.conf** désactive les unités **ssh-keygen** si **cloud-init** est en cours d'exécution.

- Pour exclure certains types de clés pour les connexions SSH, commentez les lignes correspondantes dans **/etc/ssh/sshd_config**, et rechargez le service **sshd**. Par exemple, pour n'autoriser que les clés d'hôte Ed25519 :

```
# HostKey /etc/ssh/ssh_host_rsa_key
# HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
```

Port autre que celui par défaut

- Par défaut, le démon **sshd** écoute sur le port TCP 22. La modification du port réduit l'exposition du système aux attaques basées sur l'analyse automatisée du réseau et augmente donc la sécurité par l'obscurité. Vous pouvez spécifier le port en utilisant la directive **Port** dans le fichier de configuration **/etc/ssh/sshd_config**.
  Vous devez également mettre à jour la politique SELinux par défaut afin d'autoriser l'utilisation d'un port autre que celui par défaut. Pour ce faire, utilisez l'outil **semanage** du paquetage **policycoreutils-python-utils**:

  ```
  # semanage port -a -t ssh_port_t -p tcp port_number
  ```

  En outre, mettez à jour la configuration de **firewalld**:

  ```
  # firewall-cmd --add-port port_number/tcp
  # firewall-cmd --runtime-to-permanent
  ```

  Dans les commandes précédentes, remplacez *port_number* par le nouveau numéro de port spécifié à l'aide de la directive **Port**.

Connexion racine

- **PermitRootLogin** est défini par défaut sur **prohibit-password**. Cela permet d'imposer l'utilisation d'une authentification par clé plutôt que par mot de passe pour se connecter en tant que root et de réduire les risques en empêchant les attaques par force brute.

  ATTENTION

  L'activation de la connexion en tant qu'utilisateur root n'est pas une pratique sûre, car l'administrateur ne peut pas vérifier quels utilisateurs exécutent quelles commandes privilégiées. Pour utiliser les commandes administratives, connectez-vous et utilisez plutôt **sudo**.

Utilisation de l'extension X Security

- Le serveur X des clients Red Hat Enterprise Linux ne fournit pas l'extension X Security. Par conséquent, les clients ne peuvent pas demander une autre couche de sécurité lorsqu'ils se connectent à des serveurs SSH non fiables avec le transfert X11. De toute façon, la plupart des applications ne peuvent pas fonctionner avec cette extension activée.
  Par défaut, l'option **ForwardX11Trusted** du fichier **/etc/ssh/ssh_config.d/05-redhat.conf** est définie sur **yes**, et il n'y a pas de différence entre les commandes **ssh -X remote_machine** (hôte non fiable) et **ssh -Y remote_machine** (hôte fiable).

  Si votre scénario ne nécessite pas du tout la fonction de transfert X11, définissez la directive **X11Forwarding** dans le fichier de configuration **/etc/ssh/sshd_config** à **no**.

Restreindre l'accès à des utilisateurs, groupes ou domaines spécifiques

- Les directives **AllowUsers** et **AllowGroups** du fichier de configuration **/etc/ssh/sshd_config** vous permettent d'autoriser uniquement certains utilisateurs, domaines ou groupes à se connecter à votre serveur OpenSSH. Vous pouvez combiner **AllowUsers** et **AllowGroups** pour restreindre l'accès de manière plus précise, par exemple :

  ```
  AllowUsers *@192.168.1.*,*@10.0.0.*,!*@192.168.1.2
  AllowGroups example-group
  ```

  Les lignes de configuration précédentes acceptent les connexions de tous les utilisateurs des

systèmes des sous-réseaux 192.168.1.* et 10.0.0.*, à l'exception du système portant l'adresse 192.168.1.2. Tous les utilisateurs doivent faire partie du groupe **example-group**. Le serveur OpenSSH refuse toutes les autres connexions.

Notez que l'utilisation de listes d'autorisations (directives commençant par Allow) est plus sûre que l'utilisation de listes de blocages (options commençant par Deny) car les listes d'autorisations bloquent également les nouveaux utilisateurs ou groupes non autorisés.

Modification des politiques cryptographiques à l'échelle du système

- OpenSSH utilise les stratégies cryptographiques du système RHEL, et le niveau de stratégie cryptographique par défaut du système offre des paramètres sûrs pour les modèles de menace actuels. Pour rendre vos paramètres cryptographiques plus stricts, modifiez le niveau de stratégie actuel :

```
# update-crypto-policies --set FUTURE
Setting system policy to FUTURE
```

- Pour ne pas appliquer les politiques de cryptage à l'échelle du système pour votre serveur OpenSSH, décommentez la ligne contenant la variable **CRYPTO_POLICY=** dans le fichier **/etc/sysconfig/sshd**. Après cette modification, les valeurs spécifiées dans les sections **Ciphers**, **MACs**, **KexAlgoritms**, et **GSSAPIKexAlgorithms** du fichier **/etc/ssh/sshd_config** ne sont pas remplacées. Notez que cette tâche nécessite des connaissances approfondies en matière de configuration des options cryptographiques.

- Pour plus d'informations, voir Utilisation de stratégies cryptographiques à l'échelle du système dans le titre Durcissement de la sécurité .

Ressources supplémentaires

- **sshd_config(5)**, **ssh-keygen(1)**, **crypto-policies(7)**, et **update-crypto-policies(8)**.

29.7. CONNEXION À UN SERVEUR DISTANT À L'AIDE D'UN HÔTE DE SAUT SSH

Utilisez cette procédure pour connecter votre système local à un serveur distant par l'intermédiaire d'un serveur intermédiaire, également appelé jump host.

Conditions préalables

- Un hôte de saut accepte les connexions SSH à partir de votre système local.
- Un serveur distant n'accepte les connexions SSH qu'à partir de l'hôte de saut.

Procédure

1. Définissez l'hôte de saut en modifiant le fichier **~/.ssh/config** sur votre système local, par exemple :

```
Host jump-server1
  HostName jump1.example.com
```

- Le paramètre **Host** définit un nom ou un alias pour l'hôte que vous pouvez utiliser dans les commandes **ssh**. La valeur peut correspondre au nom réel de l'hôte, mais peut également être une chaîne quelconque.
- Le paramètre **HostName** définit le nom d'hôte ou l'adresse IP de l'hôte de saut.

2. Ajoutez la configuration de saut du serveur distant avec la directive **ProxyJump** au fichier **~/.ssh/config** de votre système local, par exemple :

```
Host remote-server
  HostName remote1.example.com
  ProxyJump jump-server1
```

3. Utilisez votre système local pour vous connecter au serveur distant via le serveur de saut :

```
$ ssh remote-server
```

La commande précédente est équivalente à la commande **ssh -J jump-server1 remote-server** si vous omettez les étapes de configuration 1 et 2.

NOTE

Vous pouvez spécifier davantage de serveurs de saut et vous pouvez également éviter d'ajouter des définitions d'hôtes au fichier de configuration lorsque vous fournissez leurs noms d'hôtes complets, par exemple :

```
$ ssh -J jump1.example.com,jump2.example.com,jump3.example.com
remote1.example.com
```

Modifiez la notation du nom d'hôte uniquement dans la commande précédente si les noms d'utilisateur ou les ports SSH sur les serveurs de saut diffèrent des noms et des ports sur le serveur distant, par exemple :

```
$ ssh -J
johndoe@jump1.example.com:75,johndoe@jump2.example.com:75,johndoe@jump3.e
xample.com:75 joesec@remote1.example.com:220
```

Ressources supplémentaires

- **ssh_config(5)** et **ssh(1)**.

29.8. SE CONNECTER À DES MACHINES DISTANTES AVEC DES CLÉS SSH EN UTILISANT SSH-AGENT

Pour éviter de saisir une phrase de passe à chaque fois que vous établissez une connexion SSH, vous pouvez utiliser l'utilitaire **ssh-agent** pour mettre en cache la clé privée SSH. La clé privée et la phrase de passe restent sécurisées.

Conditions préalables

- Vous disposez d'un hôte distant avec un démon SSH en cours d'exécution et accessible via le réseau.

- Vous connaissez l'adresse IP ou le nom d'hôte et les informations d'identification pour vous connecter à l'hôte distant.
- Vous avez généré une paire de clés SSH avec une phrase de passe et transféré la clé publique à la machine distante.

Pour plus d'informations, voir Générer des paires de clés SSH .

Procédure

1. Facultatif : Vérifiez que vous pouvez utiliser la clé pour vous authentifier auprès de l'hôte distant :
   a. Connectez-vous à l'hôte distant à l'aide de SSH :

```
$ ssh example.user1@198.51.100.1 hostname
```

   b. Saisissez la phrase de passe que vous avez définie lors de la création de la clé pour autoriser l'accès à la clé privée.

```
$ ssh example.user1@198.51.100.1 hostname
 host.example.com
```

2. Démarrer le site **ssh-agent**.

```
$ eval $(ssh-agent)
Agent pid 20062
```

3. Ajouter la clé à **ssh-agent**.

```
$ ssh-add ~/.ssh/id_rsa
Enter passphrase for ~/.ssh/id_rsa:
Identity added: ~/.ssh/id_rsa (example.user0@198.51.100.12)
```

Vérification

- Facultatif : Connectez-vous à l'ordinateur hôte à l'aide de SSH.

```
$ ssh example.user1@198.51.100.1

Last login: Mon Sep 14 12:56:37 2020
```

  Notez qu'il n'est pas nécessaire de saisir la phrase d'authentification.

29.9. RESSOURCES SUPPLÉMENTAIRES

- **sshd(8)**, **ssh(1)**, **scp(1)**, **sftp(1)**, **ssh-keygen(1)**, **ssh-copy-id(1)**, **ssh_config(5)**, **sshd_config(5)**, **update-crypto-policies(8)**, et **crypto-policies(7)**.
- Page d'accueil d'OpenSSH
- Configuration de SELinux pour les applications et les services avec des configurations non standard

- Contrôle du trafic réseau à l'aide de firewalld